

Text of presentation Given by D. A. Goward

Webinar “How America is Losing the GPS War – and risking everything”

26 March 2020, Assn of Old Crows

Short clip of Khrushchev at UN clipped from <https://youtu.be/3A3TRFH6CR0>

Golly how I miss Khrushchev and that whole merry gang.

Life was so much easier when your enemies promised out loud to bury you. Now they are quietly busy getting us to bury ourselves.

Fukuyama

In 1992 Francis Fukuyama published his book “The End of History and the Last Man”. In it he argued that, with the fall of the Soviet Union, liberal democracies and free markets would spread across the face of the globe. The western lifestyle would prevail. The final form of human government had been reached, and the rest of history was just sorting out the details. So, for all intents and purposes, history had ended.

Various autocrats

Francis, you have some folks waiting who would like to speak with you.

The world, of course, is still filled with competing forces. Huge economic disparities remain, wealth and political power are concentrated within the hands of a relatively small number of elites who jockey among themselves for an even greater share. This is true within nations, and to an even greater degree between nations.

At the same time, inexpensive, widely available technologies have made populations acutely aware of these disparities fomenting resentment and discontent. Some of these same technologies have also given discontented individuals, and groups unprecedented power and the ability to act out their anger and seek retribution. They have also become the weapons of nations.

GPS started life as a weapon. Dr. Brad Parkinson's goal, as he likes to tell it, was to allow the US Air Force to put five bombs in the same hole. But there were those, including Brad, who could see its potential for peaceful benefit to mankind. They realized that, in order to realize those benefits, it had to be widely adopted and used. This meant that it had to be easily accessible and the details of signal characteristics widely known. Under their influence the United States made this information public and GPS officially became America's gift to the world. Since then other national satnav systems have followed suit so that they might also be readily adopted.

Yet, as we all know, this openness is a two-edged sword. It informs both the good guys and the bad guys. And while the good guys have done a lot of good with it, there has been some mischief, and there is potential for a lot of more.

David & Goliath

Over 3,000 years ago a shepherd boy regarded an adversary, found a fatal weakness, and used readily available technology to deliver a knockout blow.

Finding your adversary's weaknesses is the first step to protecting yourself from them, and eventually defeating them. Those who would do America harm have found many weaknesses in our technology.

Today our topic of concern is, of course, the Global Positioning System, or GPS. More generally, though, it is really about the positioning, navigation and timing, or PNT, services that GPS provides. The battle over GPS and PNT is particularly important because so many other things depend upon it. Exceptionally precise, but very weak, GPS signals have been so incorporated into networks, emergency services, industrial applications, and every mode of transportation that it is hard to estimate the devastation to our economy should it no longer be available.

Traffic clip taken from <https://www.youtube.com/watch?v=Bp1uLeExGyE>

You think your commute home from work is a nightmare? Let's take GPS out of the equation.

And that's before we talk about PNT as essential for first responders, critical applications, and networks. I hear networks are becoming important.

Jenga

GPS reliance has become so pervasive that several years ago Department of Homeland Security officials called it "a single point of failure for critical infrastructure." I suspect our friends at DHS today would tell us it is not quite as bad as it was. Still no one wants to risk turning it off for a day to see what happens.

The battle for GPS is very important but especially difficult for a number of reasons.

One is that so few know of its importance. It has been called the invisible utility, after all. And of those who do know, few know the battle is on-going and that America and the west are losing.

Rocket

Positioning, navigation and timing have been important since prehistory of course. Though in the 1980's it rocketed to prominence with the advent of GPS. And that's when the GPS and PNT war began.

As the century drew to a close more and more uses for GPS's highly precise and ubiquitous signals were found. At the same time jammer technology and use evolved.

But for a long while such things were mostly discussed in hushed tones and behind closed doors. There were reports, for example that jammers were used by Iraqi forces in 1991 during the Persian Gulf War, though little was aired publicly.

Jammer Slide

But in 1997 the Russians were so pleased with themselves that they broke the silence. The Moscow Airshow that year featured a brand-new product. It was a 4 watt GPS/GLONASS jammer with an advertised range of 200 km. The US Army was sufficiently interested that they bought 150 units to try them out.

That same year, 1997, a Presidential commission in the United States told Bill Clinton that the nation was becoming too dependent on GPS signals and recommended a backup be investigated.

1997 also saw the United Kingdom making a similar finding, though the report issued by MI-6 was in a much more engaging format.

James Bond Clip https://youtu.be/yhAh-vpuGCg?list=PLpyi-UneBu7wCzHdp-__YI9DT-dDqrRS3

While government reports and Hollywood speculations are interesting, what matters, of course, is what is happening in the real world.

But when it comes to GPS disruption, this can be difficult to discern for a number of reasons.

They are often shrugged off by users as a problem with their equipment, obstructions temporarily blocking signals, or yet another case of them not fully understanding how to use their device.

Also, those who deliberately disrupt GPS and other satnav signals generally try to avoid detection. There are a few notable exceptions (as you will see later with the Russians), but most folks try to NOT be found out.

And when organizations and governments do discover deliberate disruptions, there are a lot of incentives to keep that information quiet. Few companies are eager to reveal the weaknesses and vulnerabilities of their products and services. Few government officials want to announce yet another problem for which they don't have a solution, and don't have money, time or staff to address.

Strike3

The one exception that we know of is Europe's STRIKE3 project. They found disruption of GPS and other satnav signals, well, pretty much everywhere. Almost 500,000 instances in their samplings, about 10% of which were adjudged to be

deliberate. We all owe a debt of thanks to the European Commission for shedding light in this area where there was very little.

Aside from that stellar example, we have to rely on word of mouth and scattered media reports.

Webpage

We at the RNT Foundation are a scientific and educational charity. If you are familiar with our website and blog, you know that a big part of our education effort is being the PNT community gossip. Our blog is often all about “did you hear ...” fill in the blank.

2000 Tank

But sometimes these instances do make it into major media. This is one of the first we have been able to find. In August 2000 the Greek government sponsored a competition to determine their army's next tank. The deal was for 250 tanks and worth \$1.4 billion. Competitors included the British Challenger 2E, the US M1A1 Abrams, the German Leopard 2A5 and the French Leclerc. During the trials, the British and US tanks had embarrassing navigation problems. Later, officials discovered that GPS signals were being jammed-by a French security agency. The jammers were reportedly hidden on the firing range and remotely activated as US and British tanks were tested.

An amusing story, but emblematic of possible deeper problems. Concerns began to mount.

In 2001 the US Transportation Department's Volpe Center released a seminal report saying that America was relying too much on vulnerable GPS signals, the

Federal Aviation Administration should cancel its plans to have aircraft rely entirely on space-based navigation, that the US needed a GPS backup for other applications, and eLoran looked like a pretty good bet.

Thirteen days after the report was issued

9/11 Twin towers burning

we all received a graphic lesson about how a small group of the disenfranchised could tell the world of their grievances using readily available, unprotected technology.

Fukuyama's end of history was going to have to be put on hold for a while.

Since that time much of the attention of America's leaders has been focused on responding to bad things that have happened more than preventing them.

And since there hasn't been a catastrophic GPS disruption event, a strong, more resilient PNT architecture to eliminate it as a single point of failure has not been a priority. In fact, with the 2010 termination of the high power, low frequency, Loran PNT system in United States, our architecture has actually gotten much, much weaker.

Spoofing progress slide

At the same time, anti-GPS technology has continued on a predictable path of becoming more capable, less expensive, and easier to use.

Spoofing, or making receivers think they are in false locations, once considered impossible, or at least difficult and unlikely, has become available, almost at the consumer level. It is certainly a ready tool for intelligent users.

“Denial of service spoofing” or “smart jamming” has even been developed. With this attack, signals are transmitted that a receiver will recognize as valid, but that do not allow it to calculate a location. So the receiver won’t work, but also won’t display any warnings of a malfunction.

These developments, along with America’s general inattention, has made our adversaries, including criminals, terrorists and nation states, stronger.

While criminals and terrorists are a significant threat, adversary nations are the greatest and most existential threat to our nation. They are winning the GPS war and gaining power in other areas as a result.

We know with a certainty that Russia and China have maintained and increased their navigation warfare capability for both defense and offense. We can assume this is the case for their allies such as North Korea and Iran as well.

Worldwide Loran

Russia and China have also maintained and appear to be improving their Loran-based terrestrial PNT systems. This allows them to ensure wireless precise PNT services are available to their homelands irrespective of solar storms or enemy attack.

Both have also been active jamming western and other military forces during exercises and confrontations.

Of the two, though, Russia has been much more open about their activities.

Cell slide

Russia claims to have installed GPS jammers on 250,000 cell towers to confound US cruise missiles. It has bragged that its electronic warfare capability makes US aircraft carriers useless, and has touted an electronic shield that can jam GPS signals thousands of kilometers from its borders.

Waveform slide

Russia periodically nettles NATO exercises and its northern neighbors by jamming GPS signals. And it does this so precisely that its GLONASS satnav signals in the spectrum next door remain completely unaffected.

Russia C4ADS Slide

Russian security forces also regularly spoof GPS receivers into thinking they are at airports sometimes hundreds of kilometers from their true location. Almost 10,000 instances of this happening to ships at sea have been documented, and press reports tell us it is a regular feature of life near the Kremlin.

While this is almost certainly an anti-drone measure for VIP protection, the implications for potential offensive mischief are obvious.

China has been quieter, though some might argue even more effective, than Russia in the GPS war.

Shanghai Crop Circle Video

Russia has been able to figure out how to spoof all the GPS receivers over a broad area to the same location. China seems like they wanted to do them one better and spoof all the receivers over a wide area to random locations. Unfortunately for them, there seems to be something in either their software or equipment that tends to spoof receiver locations to points on a 200 meter wide circle centered on

the spoofer's location. You can't tell this unless you look at the spoofing activity over time. Imagine the engineer's shock when he realized that his equipment was bulls eyeing its own location!

By the way, it seems like the Chinese are doing this spoofing to hide oil imports from Iran and avoid US economic sanctions. Also, in some instances, to provide protection for VIPs as the Russians seem to do. But again, it shows what is possible for offensive operations.

More Bei Dou Slide

China has also been very aggressive fielding its BeiDou satellite navigation system. It is newer than GPS, with all the technology implications that brings, and is rapidly achieving a physical dominance in the skies of much of the world.

BeiDou+ GLONASS

China has also announced with Russia intentions for greater cooperation between BeiDou and Russia's GLONASS satnav system, suggesting that the two could merge into a mega constellation. One that, numerically at least, would surpass a combination of GPS and Europe's Galileo satnav constellations.

And at last year's Stanford PNT Symposium a representative from China announced their intent to launch multiple new PNT systems for operation nationally and globally. Among those are geostationary PNT satellites, and a Low Earth Orbit PNT constellation broadcasting new L Band signals. The entry proposal for the LEO effort now with the ITU for consideration is for 120 new satellites at 700 km altitude. Such a system could provide more accuracy and resilience,

presumably broadcasting at higher power than today's Medium Earth Orbit constellations like GPS.

China Architecture

China's most significant advantage is its commitment to a comprehensive PNT architecture that includes multiple diverse sources from both space and terrestrial. PNT from satellites at GEO, MEO, and LEO, and from the ground with enhanced Loran, WiFi and cell ranging, advanced inertials, and so on, including systems that have yet to be developed are all part of the plan.

Such a system of systems available to the entire nation, not just military forces, will provide a degree of national resilience and robustness not found anywhere else in the world. Certainly, an economic, military, and societal advantage for China.

DoD Strategy

It is true that In the US the Air Force NTS-3 program is examining enhancing GPS from geostationary orbit. And the US Army has a project with the University of Texas to investigate "leveraging thousands of still-to-be-launched LEO broadband communication satellites" for PNT.

These are both worthy efforts, but they do not approach the kind of integrated space/terrestrial PNT architecture China is developing, and that is called for in the US Department of Defense PNT Strategy.

Should we take heart that our Department of Defense is at least talking about a strong, resilient architecture?

Perhaps. But before we get carried away with optimism, we should remember two things.

First, government strategies are often published as a way of trying to avoid real action on an issue. GPS III and its related programs are very expensive. There are undoubtedly a lot of incentives for many in the DOD to focus on GPS III exclusively and defer or ignore other PNT efforts. I understand that far too many people in the Pentagon have sold GPS III as the program that will solve all PNT problems. They certainly would not want any alternate PNT programs or systems questioning that, or competing for funds.

The second reason we shouldn't be too optimistic, is that, even if DOD does build out the multi-level architecture called for by its strategy, it is unlikely to make non-military American users, critical infrastructure, networks, and so on any safer. The DOD strategy complains that civil use of GPS has limited their ability to use it as a military tool. Future DOD systems, it promises, will be "increasingly classified" and therefore not available for civil use.

So, what does all this mean in this undeclared, low level, GPS and PNT war that is taking place pretty much out of sight?

It means that America is at a major disadvantage at all three levels of warfare, tactical, operational, and strategic.

Drone spoof 2011.

It means that the odds can be stacked against our forces in specific tactical engagements. Iran has been particularly good at demonstrating this.

In 2011 they claimed to have spoofed a CIA drone operating next door in Afghanistan into landing at one of their airbases. At the time US government officials first said that spoofing was not possible. Then after Todd Humphries at the University of Texas demonstrated how to do it, they said that spoofing was not what happened in this case. Yet the Iranians clearly had the drone and these government officials offered no alternative explanation for how they got it.

Navy Boat map

There is also reason to believe that it wasn't a coincidence two US Navy boats wandered into Iranian waters and were captured just after President Obama's nuclear deal with that nation,

Obama/seizure

AND on the day of his last State of the Union address. I have been told by a US government official that the boats were not spoofed. Yet the boats were clearly captured in Iranian waters far from where they their crews thought they were, and the Iranian Navy was waiting for them in force. This government official offered no alternative explanation for how these boats got so far off course in an unlikely direction.

Drone shoot

And there is reason to believe that, in the most recent military confrontation between the United States and Iran, spoofing was used to move a US surveillance drone into Iranian airspace and enable Iran to shoot it down with impunity. I have not bothered to discuss this with any government officials.

Syria slide,

And of course, every week we see other, less surprising cases of GPS disruption being a problem for American forces that are acknowledged by US officials.

At the tactical level of war, our adversaries are doing very, very well.

Russian Jamming equipment

At the operational level of war, the goal is to prepare the battle space to your advantage. Russian military doctrine holds that when their forces go into battle, every signal from space will be denied them. As a result, they are fully prepared to ensure these signals are also denied their opponents. They are also reported to have a mobile terrestrial system called Skorpion to provide their own forces the wireless PNT they need in battle.

But to be honest, shaping the battle space to disadvantage those who rely upon weak GPS signals is not difficult. It is within the grasp of virtually every nation.

Sen Sasse

It is at the strategic level of war, though, that in my view, America's adversaries are making the greatest strides.

Every time Russia jams NATO forces, Iran spoofs a drone, or China interferes with GPS near the Spratly Islands, they are enhancing their global stature and diminishing that of America and the West.

They are sending a set of clear, unambiguous messages.

To America they are saying

With the flip of a switch we can neutralize a major component of your military forces.

Without firing a shot, we, or one of our proxies not traceable to us, can strike at the heart of your homeland, cripple your economy, and seriously undermine the legitimacy of your government.

And, by way, if you decide to respond in kind, our homelands are not nearly as vulnerable as yours because we have terrestrial systems.

To the rest of the world they are saying

America's much touted "gift to the world" in GPS is not worth as much as they claim. And using it might cause you trouble. Use ours also, or, even better, use ours instead.

And they are saying America and western systems are not as powerful and important as they might seem. They are vulnerable and easily defeated.

Ally with us. We are better partners.

These messages are delivered implicitly through their actions, and sometimes, a bit more overtly

Putin Slide

But they are generally effective, because they contain so much truth.

For too long America, and Europe for that matter, have had an unhealthy fixation on PNT satellites in medium earth orbit, when we should have been focusing on a robust and resilient PNT architectures to protect our populations. We have put all our eggs in a very vulnerable basket.

Yet there are some encouraging signs in America and the west. Europe is contracting for a GNSS interference detection network. It has admitted that

satnav signals alone are not sufficient for safety critical applications. And is exploring what that means in terms of systems.

The United Kingdom is establishing a timing center with the goal of protecting itself from satnav disruptions.

Here in the US the Congress has funded a demonstration program for technologies that might serve as a backup for GPS. It has also mandated a wireless terrestrial backup system for GPS time services be in place by December of this year. And the president has issued an Executive Order on Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services. While this order increased overall awareness of the issue, it unfortunately deferred most actions for a year or more to provide the opportunity for “more study.”

PTA

Should more be done? We think so.

Our vision is a stronger, safer America. One with transportation systems, technology, and our way of life not constantly in danger from solar storms and a wide variety of malicious actors.

To get there the RNT Foundation advocates and echoes the President’s Positioning, Navigation, and Timing Advisory Board call for a holistic approach to the problem. An approach that involves protecting the frequencies, toughening users, and augmenting GPS signals.

Protecting the frequencies means looking for disruptions, stopping them, and leveeing sanctions to prevent it from happening again. None of which our government has shown much interest in doing.

Toughening receivers means encouraging, and sometimes requiring, use of existing hardware and software that helps resist many forms of interference. It's available, it just costs a bit more.

Augmenting spaced-based capabilities with a high-power terrestrial system is undoubtedly the single most effective thing that could be done, though.

Having a set of terrestrial signals everyone can rely upon will protect GPS satellites and signals by making them less attractive targets. Why bother to attack or disrupt if it will have only minor impacts to users?

And receivers that use both space and the terrestrial system will be tougher. The eLoran system that the US government has announced twice that it would build for this purpose has a signal received at 1.3 million times the strength of GPS. And terrestrial signals could be coded and authenticated to further increase security.

Properly augmenting GPS with terrestrial signals could make users virtually bullet-proof.

Architecture

In fact, we argue that America needs a comprehensive PNT architecture, like the one China has announced. This will help ensure users have services when and where they need them. Establishing a terrestrial augment/backup for GPS is just step one.

But there are significant challenges here. Not technical because the terrestrial systems under discussion are mature technologies, which is not to say outdated. Just like the telephones, radar, and televisions we use now are much more advanced than those of 20 years ago, powerful wireless terrestrial navigation and timing systems have advanced and modernize as well.

And the challenge is not money. We spend over a billion a year on GPS. We have seen estimates that less than \$50M a year would be needed for the government to have a full-up and capable terrestrial system. A small amount compared to what we are spending elsewhere. A mere pittance compared to what it would cost us if GPS were ever to have a significant outage.

The challenges are, and always have been, political.

GPS III Costs

GPS was, and now GPS III is, very expensive. So the program wars in the federal government limit discussion of any shortcomings and the need for other systems. Much of this is likely unconscious and unintentional. But look at all the hype, for example, about GPS III. While we absolutely do need to refresh the constellation, the sound bites touting GPS III make you think it is solving major problems. In fact, the improvements over what we have now are very minor.

And we are also challenged by the fact that nothing really bad has happened... yet. On the whole, GPS service has been incredibly reliable.

In America we often seem to have difficulty doing what we know we should to prevent bad things from happening.

New London School

The need to add a malodorant to natural gas so leaks could be quickly detected was debated for decades. That is until 1937, when an explosion killed hundreds of school children in New London, TX.

NOLA Flood

We knew the levees in New Orleans were not adequate long before Katrina.

Twin Towers

For years aviation experts said we should harden cockpit doors the way the Israelis had to prevent hijackings. But we didn't do that until after 9/11.

Covid-19

And we knew that a world-wide pandemic would someday be a problem. Yet despite being the richest, and allegedly most advanced, nation on the planet, we were complacent. Not only did we fail to prepare, but we started disassembling the structures that could keep us safe.

Much like we did with navigation and timing when we shut off the old Loran-C system in 2010.

Uncle Sam

If we are to prevent another disaster, one that could have at least the same impact as the current pandemic, it is up to all of us to urge preparation and prevention. To tell the story and demand that our leaders work to prevent bad things from happening, rather than just reacting after the fact.

The first steps of this are putting a federal official charge, and ensuring we have a terrestrial system to complement our assets in space.

Cyber slide

We know the things that need to be done. It is just a matter of finding the political will to do them.

As things are now it is not too much to imagine that one day we might wake up to find that Mother Nature has sent a solar storm to again remind us of how tenuous life is on this planet. Or that a nation, terrorist group, or transnational criminal organization has turned our single point of failure into a knife at our throat. Or that we are facing the next disaster from which we might need decades to recover.