How the West is Losing the Navigation and Timing War

Dana Goward, President of the Resilient Navigation and Timing Foundation, shares his views and breaks down his keynote presentation from the recent International Navigation Conference.

- **Thousands of ships at sea report their positions as being at airports**
- **China announces plans to add LEO PNT satellites and new technologies to their already-impressive terrestrial and MEO PNT capabilities**
- **Syria is 'the most contested electronic battlefield on the planet'**
- **Iran may well have spoofed another US drone**

In an age of nuclear, biologic, and chemical weapons, it is hard to imagine a global conflict on the scale of the last world war.

Yet huge economic and social disparities remain between nations. Tribalism, national pride, and fear of "the other" are all too common. And so, struggles between nations and groups of nations continue. Perhaps more quietly and subtly, but nevertheless very much in earnest.

In every way, each side is looking to exploit their adversaries' weaknesses. For the last forty years or so, adversaries of the West have found an easy target in satellite-based positioning, navigation, and timing (PNT). A combination of vulnerabilities and broad dependence have cause US security officials to call it "a single point of failure for critical infrastructure."

Of course, PNT has been important since prehistory. Nations have long sought advantage over each other by improving their own capabilities and, at times undermining those of their adversaries. The British weren't the only ones desperately searching for a way to find longitude in the early 1700's, for example.

This war for navigation and timing was greatly accelerated, though, with the advent of America's Global Positioning System (GPS) and Russia's GLONASS, both of which became fully operational in 1995.

JAMMING

The exceptionally weak nature of these signals, along with the tremendous military and civil advantages they provided, made them targets very early on. As one example, Iraqi forces were reported to have employed jammers to help protect high value targets in the 1991 Persian Gulf war, even though U.S. forces had only a limited number of receivers and a partial constellation to work with.

Such things were mostly discussed in hushed tones and behind closed doors. At least until 1997 when the Russian company Aviaconversia offered a portable GPS/GLONASS jammer for sale at the Moscow Air Show. The 4w jammer reportedly had a range of 150 km to 200 km.

The United States Army was sufficiently interested to place an order for almost $200,000.

In the years that followed, both global navigation satellite system (GNSS) technology and the technologies to disrupt it evolved.

For years reports of disruptions, at least in the public sphere, were rare. Though occasionally they would make it into the popular media.

One of the first was actually between frenemies within the West.

In 2000 the Greek government held a competition for procurement for a new army tank. The contract was to be for 250 tanks and estimated at $1.4 Billion. Competitors included tanks from Germany, France, Britain, and the United States. The British and US tanks performed poorly during the trials. It seems a French security agency had hidden GPS jammers on the range and remotely activated them whenever the British and American tanks were on the field.

Jamming weak GNSS signals quickly evolved from the province of elite military electronic warfare units to something easily available to anyone with $35 and an internet connection.

THE ADVENT OF SPOOFING

As jamming became more prevalent, a second GNSS weakness was eventually revealed – spoofing, or deceiving receivers with potentially hazardously misleading information.

In retrospect, this development was probably inevitable.

As part of encouraging wide use and adoption of GPS, the United States made its signal characteristics public knowledge. Thus, GPS became "America's gift to the world."

Naturally, other GNSS operators followed suit to encourage broad adoption of their signals.

These efforts were wildly successful. GNSS signals have been adopted for an incredible array of previously unimagined uses. But making the details of the signals public, in addition to making the incredibly useful, also accelerated the ability of bad actors to be able to send false signals.

The first public claim of this was in 2011 when Iran came into possession of a US surveillance drone that had been operating next door in Afghanistan. Iranian engineers said they had transmitted false GPS signals to the drone to cause it to cross the border and land at an Iranian airfield.

US officials at first said it couldn't happen. Several months later Todd Humphries at the University of Texas essentially said "sure it can – watch" and spoofed a drone in front of the press in the university's stadium.

Since then, spoofing technology has become cheaper, more capable, and easier to use. A predictable technological progression. Small spoofing devices are now readily available, inexpensive, can imitate multiple constellations at once, and can be operated by any moderately informed user.

While jamming and spoofing by individuals and groups are a serious threat, it is the West's national adversaries that should be of greatest concern.

They are winning the navigation and timing war and gaining power in other areas as a result.

RUSSIA AND CHINA ADVANCING

We know with 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.

Russia and China have both 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 actively jamming western and other military forces during exercises and confrontations. Each has also developed aggressive capabilities to spoof GNSS signals over wide areas.

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

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 aircraft carriers useless, and has touted an electronic shield that can jam GNSS signals thousands of kilometers from its borders.

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

Russian security forces also regularly spoof GPS receivers into thinking they are at airports tens 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 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 navigation and timing war.

There is evidence that China has improved upon Russia's ability in

wide-area spoofing. Rather than cause all impacted receivers to report that they are at the same remote location, China's system seems to move them each to different, semi-random locations (though something in their algorithm seems to favor points that form circles over time).

China's BeiDou satellite navigation system is newer than GPS, with all the technology implications that brings, and is rapidly achieving a physical dominance. More BeiDou than GPS satellites are visible in the skies of 130 of 195 countries.

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

And at the recent Stanford PNT Symposium a representative from BeiDou confirmed China's intent to launch multiple new PNT systems for operation nationally and globally. Among those is a Low Earth Orbit (LEO) constellation broadcasting new L Band signals. The entry proposal now with the ITU for consideration is for 120 new LEO satellites at 700 km altitude. Such a system could provide more accuracy and resilience, presumably broadcasting at higher power than today's MEO GNSS constellations.

China's most significant advantage is its commitment to a comprehensive PNT architecture that includes multiple diverse sources from legacy Loran to systems that have yet to be developed.

Such a system used by the entire nation, not just military forces, will provide a degree of national resilience and robustness not found elsewhere. Certainly, an economic, military, and societal advantage for China. An advantage in the navigation and timing war, and its quest to become the next sole global superpower.

THE WEST MOSTLY RETREATING

In 1997 a presidential commission told Bill Clinton the U.S. was likely becoming too dependent on GPS signals. This was confirmed in 2001 by a seminal report by the US Department of Transportation's Volpe Center. It said that GPS signals were incredibly vulnerable, and the nation must cancel its plans to have aircraft rely entirely on space-based signals for navigation. It said that other transportation modes, and many non-transportation interests, required a complementary and backup capability for GPS. It also said that eLoran looked like a good bet to be that backup and should be further investigated.

Unfortunately, thirteen days after the report was issued, the World Trade Center towers fell. Leaders' attention was diverted elsewhere. Even so, in 2004 President Bush issued an order, which is still in effect, to implement a backup capability for GPS against the inevitable day it was no longer available. This was described as a national economic and security necessity.

Despite this knowledge and mandate, the United States and the West proceeded to reduce its PNT capability, rather than enhance it. Most notable were the termination of the U.S. and Canadian Loran systems in 2010, and Europe's in 2015. Massive blows to what should have been expanding and increasingly robust PNT architectures.

The result has been that the West's already dangerous over-dependence on space based PNT has been tremendously exacerbated.

Compounding this challenge in many western nations is the lack of governmental leadership for civil PNT issues. The United States is a good case study.

The U.S. Department of Defense has long been aware of GPS vulnerability and has actively pursued remedies. Yet over 99% of GPS users have nothing to do with the military. There are no national efforts to protect their interests and users.

Nor will these users benefit from defense efforts. That department has declared that civil use of GPS has hindered its operations. Therefore, future defense PNT efforts and systems will be "increasingly classified" and therefore not available to civilians.

The U.S. Department of Transportation is tasked with leadership of civil PNT issues, but only lightly so. There is a broad lack of recognition and support for this role across the bureaucracy and within Congress. This has meant that the department has been unable to garner support for even minor efforts such as funding to monitor and report on the health and quality of civil GPS signals. The department has here-to-fore not even attempted other efforts to improve the nation's PTN architecture – even those mandated by presidential order.

AND SO GOES THE WAR

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

Because PNT is so critical to military and civil activities, it means that the West is at a major disadvantage at all three levels of warfare - tactical, operational, and strategic.

TACTICAL LEVEL

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

In addition to spoofing the CIA drone in 2011, there is also reason to believe they bested the US in two subsequent cases.

Many believe 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. It also happened to be on the day of his last major policy speech. US officials have privately commented that spoofing was not a factor in this incident. But as was the case for the drone in 2011, they offered no alternative explanation for what happened.

There is also 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.

And of course, every week we see other, less surprising cases of GNSS disruption being a problem for western forces operating in the eastern Mediterranean and middle east.

At the tactical level of war, the West's adversaries are doing very, very well.

OPERATIONAL LEVEL

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 to power their systems in battle.

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

STRATEGIC LEVEL

It is at the strategic level of war, though, that the West'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 the west 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 hearts of your homelands, cripple your economies, and seriously undermine the legitimacy of your governments.

And, by way, if you decide to respond in kind, our homelands are not nearly as vulnerable.

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 the West and its 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. Sometimes a bit more overtly as when the front page of the Moscow Times read "The Kremlin Eats GPS for Breakfast!"

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

ARCHITECTURE vs SYSTEMS

For too long the West has had an unhealthy fixation on PNT satellites in medium earth orbit, when we should have been focusing on a robust and resilient PNT architecture to protect our populations. We have put all our eggs in a very vulnerable basket.

Yet there are some encouraging signs.

Europe is contracting for an interference detection network. It has admitted that GNSS alone is not sufficient for safety critical applications. And it is exploring what that means in terms of systems.

The United States is in the early stages of figuring out how to build a terrestrial timing backup. One that can be expanded into a navigation system. This is much more of a political problem than a technical one. That means the process is much more complex and uncertain.

Let's hope that these measures continue, and more are undertaken to protect GNSS signals, toughen receivers, and provide difficult to disrupt terrestrial augments.

Let's hope that these are not too little too late.

As things are now, it is not too much to imagine that one day soon we might wake up to find that a nation, terrorist group, or transnational criminal organization has turned our single point of failure into a knife at our throat.

Mr. Dana A. Goward is the President of the Resilient Navigation and Timing Foundation. He is a member of the US National PNT Advisory Board and formerly served as the maritime navigation authority for the United States.