ASIA PROGRAMME

THE CHINESE GLOBAL POSITIONING SERVICE AND THE CONVERGENCE BETWEEN ELECTRONIC WARFARE AND CYBER ATTACK

BY **EMMANUEL MENEUT**
PH.D, LECTURER AT THE CATHOLIC UNIVERSITIES

MAY 2020

ASIA FOCUS #141

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

The digital infrastructure for maritime and air navigation security contributes to diffuse a global common : the Global Positioning Service (GPS) through enhanced connectivity. This global common is dual, both essential to military forces and civilian activities, especially transportation. As a consequence, it is a "perfect target" for hybrid warfare. Moreover, the securization of this infrastructure rests either on an hegemon which provides security for all users or the diffusion of multiple positioning systems from great powers which are interoperable. The issue would be an increase of the cost of the positioning service and the nature of the security regime. Indeed, the securization process requires either trust among a set of countries to diffuse only one digital infrastructure with financial gain for all or an anarchical security regime between countries and a set of costly inter-operable systems. In a unipolar world, the security regime would be close to a stable hub & spoke alliance with a keystone country as the main security provider. On the contrary, in a multipolar world each great power provides a "global positioning service" as a lever to balance power politics of others through shifting alliances. It is a classical balance of power phenomena. Actually, GPS are provided by multinational companies but in last resort it is controlled by the defence and security state apparatus. The US GPS provide positioning information with a three meters precision but it may be decreased on any area by a simple decision from the Pentagon. It is the main driver for the development of the Chinese GPS "Beidou" through its ecosystem of more than 120 companies closely linked to the party state. The Beidou system is fully operational at a global level since 2020. We are analyzing the current features of the rising GPS rivalry between these two great powers in order to illustrate the security dilemma in the technological field.

GENEALOGY OF THE GPS AND ITS RISES AS A GLOBAL COMMON

At the origin: the availability of a military navigation service to the civilian sector for security purpose

Following the destruction by the Red Army fighters of Korean Air Lines flight KAL007 when it went off course near the Sakhalin Island on August 31, 1983 ; president Reagan offered free use of the American global positioning systems of its armed forces through its standard positioning service to all users on a continuous, worldwide basis, for the indefinite future, free of any direct user charge[1]. In December 1993, the GPS satellite constellation was declared operational for civilian use. Moreover, the "selective availability" feature enables the US government to deny the GPS to other armies via jamming within the operations theater while civil users outside the battlefield are not denied the positioning service[2]. This point is essential because American smart weapons used intensely positioning coordinates and navigation systems. « The pace of operations requires constant access to data in real time »[3]. Global communications make possible the US concept of networked warfare, which is a strategic advantage of the American armed forces against any adversary anywhere. The conventional military advantage in precision weaponry is at the heart of the global security provider status of the American armed forces and it requires the control of an efficient GPS. This global positioning service rests on the hegemonic position of the US in the field of security, and it is a key lever to maintain this status. This standard positioning service for civilian users is also a key strategic advantage for the US forces, however it is vulnerable to electronic warfare and jamming. It is a dual global service.

The GPS rises as a global common

Today, civilian uses of US GPS are growing rapidly. This is largely due to the quality of the US GPS and its global nature through connectivity. GPS uses improves transportation

1 (VOLPE, 2001) John A VOLPE, (29/8/2001), Vulnerability assessment of the transportation infrastructure relying on the global positioning system, National Transportation Systems Center for the US department of transportation
2 (VOLPE, 2001) John A VOLPE, (29/8/2001), Vulnerability assessment of the transportation infrastructure relying on the global positioning system, National Transportation Systems Center for the US department of transportation
3 (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy

means and increases their operational efficiency. Its ease of use and the rapidly decreasing user equipment cost increases the amount of access, it is the main drivers of this rapid GPS diffusion process.

For example, the US GPS has become the normal means for shipping positioning and timing in the maritime sector[4]. Other civilian sectors are also concerned. With more technology in cockpits, passenger airplanes are increasingly dependent on GPS navigation. When approaching airports, GPS navigation in modern days is the equivalent to radio navigation and air-to-ground based navigation systems of the past[5]. All airports with commercial flights still have radio and other instrument landing system's pilots use when approaching the runways[6]. However, in the current state of affairs of civilian aircraft, the GPS navigation is becoming the dominant source of information for positioning and timing. As radio navigation aid, GPS has the capability to serve as the only navigation system that users need to employ.

Aircraft crews depend on Flight Management Systems (FMS) through all phases of their flight. Using high-powered computers to manage navigation, atmospheric and fuel data flows. The FMS allows pilots to optimize both safety and economy of the flight. Newer FMS navigation systems rely solely on GPS to determine aircraft position and have no need to continuously monitor omnidirectional radio stations on ground. It is potentially a huge source of maintenance cost reduction of ground infrastructure and the opportunity to cover large area underequipped.

More generally, GPS systems have become nearly ubiquitous in the modern economy, deployed in smartphones, cars, and industrial control systems. The US electric grid, for example, uses GPS for a variety of purposes[7].

This is the genealogy of a global information infrastructure which becomes a global common. The low-cost access and the maintenance cost decreased entailed rapid diffusion following a classical “S” curve with a hegemon country, the US, as the security

[4] (GRANT et al., 2009) Alan GRANT, Paul WILLIAMS, Nick WARD, Sally BASKER, (April 2009), GPS Jamming and the impact on maritime navigation, Journal of navigation volum 62 n°2, pp 173-187
[5] (NILSEN, 2018) Thomas NILSEN, (2 November 2018), Pilots warned of jamming in Fin mark, The Barents observer
[6] (NILSEN, 2018) Thomas NILSEN, (2 November 2018), Pilots warned of jamming in Fin mark, The Barents observer
[7] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy

provider which bears the security cost of this global common. GPS technology had increased user's ability to exploit the ocean and air spaces much more efficiently and it rises the intensity of exchanges and mobility. Thus, raising the political question of security. Actually, as GPS further penetrates into the civil activities, it becomes a tempting target that could be exploited.

THE VULNERABILITY OF THE GPS SHIFT THE POWER POLITICS ISSUE : THE SPOOFING ATTACK AND THE INCREASE OF UNCERTAINTY ON THE GPS SERVICE RELIABILITY

From a dual GPS to a strategic target at the centre of hybrid warfare

Electronic warfare significantly increases the ability to jam the positioning service. It is part of the technical opportunity to challenge the US dominance in precision weapons and undermined the US airspace strategic advantage[8]. During the last decade, the Russian military forces have made massive investments in electronic warfare[9]. 25 000 Russian radio waves cell towers had been installed with GPS jammers to thwart US cruise missiles[10]. In a war, sabotaging the GPS systems would deal an enormous blow to its adversary's armed forces, which would have to rely on inferior tools : Warship would traverse oceans less accurately and fighting aircraft would struggle to locate friendly ground forces and to locate targets[11].

The strategic issue with electronic warfare is you can't measure it[12]. The first difficulty raises in the estimate of who is able to disrupt ship and aircraft positioning and their impacts on ports and airports activities. In the conventional field, it is easy to determine the state of an adversary's level of capacities, you count military planes and ships and you know what your adversary is up to. But, in the electronic warfare, you don't have that option. You don't know when they've achieved a strategic breakthrough. If your strategy

[8] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy
[9] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy
[10] (US PNT advisory board, 2018) US national PNT advisory board, (17 May 2018), GPS Russia undermining confidence in GPS
[11] (BRAW, 2018b) Elisabeth BRAW, (17 December 2018), The GPS wars are here, Foreign Policy
[12] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy

to defend any allied is based on a rapid reinforcement of your already deployed forces, ports, airports and positioning service are essential infrastructure and must be protected. As a consequence, the position digital systems are essential to the success of your armed forces and the credibility of the hub and spoke alliances at the centre of your status of the global security provider[13]. The growing ability of Russian and Chinese forces to blind or disrupt digital communications might help level the playing field when fighting against a superior conventional foe[14]. While this arms race continues, the major shift concerning the international security regime is occurring in the civilian usage of the GPS services because of its dual usage.

Indeed, a major blow of the GPS would also be a blow for all the civilian ships and aircrafts:

- The cargo ship that carry 90 % of global trade could find themselves travelling in the wrong direction. They could collide with rocks or other ships
- Civilian airplane pilots would have to resort to less precise manual navigation and landing procedures.

Most ordinary, smartphone users would find themselves baffled, with deliveries loss, trips delayed, etc. Nine in ten smartphone owners use GPS supported apps[15]. "Everyone should accept the fact that many of today's conveniences are, in fact, a luxury and learn how to live without them in a pinch[16]." Electronic warfare opens new kind of "hybrid warfare". In this kind of conflict, disruption of daily life is a crucial part of hybrid warfare. By causing society to grind to a halt, or even just making daily services such as food, medicine or fuel supply, sewage, news media, or the Internet working poorly, an adversary can dramatically weaken the target country without moving a single soldier. This permanent threat is structuring international relations between great powers and the international security regime. During NATO's Trident juncture exercise, held in Norway in 2018, GPS signals failed. Civilian airplanes were forced to navigate manually and ordinary citizens could no longer trust their smartphones.

[13] (BRAW, 2018) Elisabeth BRAW, (5/11/2018), there's non plan B for port security : privatization and automation have left global shipping fatally exposed, Foreign policy
[14] (MCLEARY, 2015) Paul MCLEARY, (21 October 2015), Russia's winning the electronic war, Foreign policy
[15] (BRAW, 2018b) Elisabeth BRAW, (17 December 2018), The GPS wars are here, Foreign Policy
[16] (BRAW, 2018b) Elisabeth BRAW, (17 December 2018), The GPS wars are here, Foreign Policy

The vulnerability to the linkage of low cost electronic warfare and cyber attack

The growth of the number of activities using the GPS increases the level of reliance on such systems for position and navigation over the past decade (2000-2010)[17]. Actually, in the 1990s, the integration of GPS time and position data with long-standing VHF radio technology enabled the development of automatic identification system (AIS). Usually, ships use a positioning system based on small fitting transponders to vessels that continuously transmit a signal which alert other vessels with a receiver to the presence of that vessel. Its primary purpose was to allow vessels to see who else is operating in their immediate vicinity so as to prevent collisions with a line of sight range of 15 miles. With technological improvements it went global in 2002, primarily with the help of the GPS signal which suppressed any line of sight range. All passenger ships and other commercial vessels over 300 tons should carry transponder and receiver. It concerned around 100 000 ships. This navigation service increases port efficiency and tracking of a ship. In the same time, it creates new opportunity to target ships. In 2011, the oil tanker Enrico Ievolli, nearby Somalia shores, was easily hijacked by terrorists. They were able to track its position through the hacking of its AIS/GPS. When the tanker was at its furthest point from any armed forces, terrorists launched their attack successfully[18].

Less than 10 years after this event, rose another kind of attack targeting Maersk, a cyber attack. Maersk is a worldwide maritime operator ranging from ports logistics to oil drilling, in 574 offices, in 130 countries around the globe. This maritime giant is responsible for 76 ports on all sides of the earth, and nearly 800 seafaring vessels, including container ships carrying tens of millions of tons of cargo, representing close to a fifth of the entire world's shipping capacity. In June 2017, within half an hour, all computer screens went black. Disconnecting Maersk's entire global network took the company's IT staff more than two hours[19]. For 10 days, 80 % of its business processes, were held manually knowing that 15 000 containers enter into a port every 15 minutes.

[17] (PORT TECHNOLOGY, 2010) PORT TECHNOLOGY, (14 December 2010), *GPS Jamming and its impact on maritime safety*

[18] (BURTON, 2014) Ryan BURTON, (May, 2014), *Cyber sécurité et marétique, un enjeu européen ?*, CARGO MARINE, Centre d'études stratégiques de la marine

[19] (GREENBERG, 2018) Andy GREENBERG, (August, 2018), *The Untold Story of NotPetya, the Most Devastating* Cyberattack in History, WIRED, at url : https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

The overall IT infrastructure : 4 000 servers, 45 000 PCs and 2 500 softwares were manually reinstalled. It was a financial loss of $ 300 million in annual sales[20].

This case illustrates the potential for a permanent disruption of a key maritime operator, by coupling the ability to track its vessels and to destroy the integrity of its position data. It will also destroy its ability to coordinate its activities all over the world with the help of the position data. By targeting few key maritime operators, it is the ability to disrupt most of the maritime sector.

Indeed, any global position satellite system, like the US GPS, is vulnerable to electronic warfare. The GPS signal is vulnerable to radio frequency interference. It offered the possibility for targeting by an electronic warfare weapon. Moreover, potential attacks cover the spectrum from jamming to spoofing of GPS signals[21]. Spoofing means inducing a GPS receiver to produce misleading position information to users. Spoofing can supply the wrong position and time information into multiple on board electronics and the company's information systems to disrupt global businesses processes. Indeed, uncertain information destroy the trust into all the information systems. As a consequence, users cannot rely on the digital tools, to support their activities. GPS spoofing requires equipment capable of cheating the GPS signals by sending dedicated signals that the GPS will interpret as genuine and consequently will show a wrong position[22]. Spoofing will provide positioning service preventing receivers to compute the real position and leading to wrong position[23]. Spoofing provide a strategic advantage in case of conflict. Spoofing activities had been reported by aviation and maritime activities in the Baltic and Black Sea and in Ukraine and Turkey[24]. Between February 2016 and November 2018, the think tank C4ADS recorded 9 883 spoofing instances affecting 1 311 vessels[25]. With the advent of software defined radios systems, spoofing GPS signals has become both easy and cheap.

[20] (AUFFRAY, 2018) Christophe AUFFRAY, (January2018), *Les 10 nuits en enfer de Maersk pour réinstaller 4 000 serveurs et 45 000 PC*, ZDNET
[21] (Port technology, 2010) PORT TECHNOLOGY, (14 December 2010), *GPS Jamming and its impact on maritime safety*
[22] (WINGROVE, 2018) Martin WINGROVE, (15 may 2018), *How can shipowners protect against GPS jamming and spoofing*, Rivera Maritime
[23] (AIRBUS, 2019) AIRBUS (September, 2019), *GNSS interference, Safety first, n°29*
[24] (US PNT Advisory Board, 2018) *US national PNT advisory board*, (17 May 2018), *GPS Russia undermining confidence in GPS*
[25] (GROLL, 2019) Elias GROLL, (3 April 2019), *Russia is tricking GPS to protect Putin, Foreign Policy*

A 1 kW portable jammer can block a GPS receiver from as far away as 80 km[26]. GPS jammers are radio frequency transmitters that intentionally interfere, jam or even block communications tools such as mobile phones, text messages, GPS systems and WIFI networks. According to C4ADS , the cost of equipment used to spoof a GPS signal is about $ 350, down from about $ 10 000 a few years ago[27]. The use of low cost mobile electronic warfare systems is a strategic advantage to defeat mobile communication signals[28]. More than 40 types of electronic warfare equipment and control system are used by armed forces[29]. The European commission says they have identified over 140 000 unique electronic signatures for GPS jammers in Europe. Electronic warfare and cyber weapons enable any actors with sufficient capacities to hack a port's operator position systems and business information systems[30]. Additionally, the increased sophistication and scale of spoofing of GPS signals, seen recently in the maritime domain, indicate how adversary techniques are rapidly evolving[31].

The spoofing feature : the target is not the GPS signal but the reliability of the service covering area and nodes of the transportation network

When the GPS signal is spoofed, it is all the systems which used this signal as an input which become unreliable. If position data lose their integrity and became uncertain, the GPS is unreliable and it raises the risk level of a collision either with the relief or with another ships[32]. Uncertainty on the quality and integrity of GPS is the result of spoofing. Actually, the result of such signal interferences could be the presentation to the GPS user of hazardously misleading information for navigation and situational awareness[33]. For example, the GPS receiver of a ship is moored, it goes haywire placing the ship few miles away on the path of a nearby ports. A mobile GPS spoofing device may manipulate global navigation systems on a scale far greater than previously understood[34].

[26] (NILSEN, 2018) Thomas NILSEN, (2 November 2018), Pilots warned of jamming in Fin mark, The Barents observer
[27] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy
[28] (NILSEN, 2018) Thomas NILSEN, (2 November 2018), Pilots warned of jamming in Fin mark, The Barents observer
[29] (NILSEN, 2018) Thomas NILSEN, (2 November 2018), Pilots warned of jamming in Fin mark, The Barents observer
[30] (BRAW, 2018) Elisabeth BRAW, (5 November2018), there's non plan B for port security : privatization and automation have left global shipping fatally exposed, Foreign policy
[31] (COOPER, 2019) Pete COOPER, (2019), Aviation cybersecurity, Atlantic Council
[32] (Port technology, 2010) PORT TECHNOLOGY, (14 December 2010), GPS Jamming and its impact on maritime safety
[33] (GRANT et al., 2009) Alan GRANT, Paul WILLIAMS, Nick WARD, Sally BASKER, (April 2009), GPS Jamming and the impact on maritime navigation, Journal of navigation volum 62 n°2, pp 173-187
[34] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy

The GPS system is vulnerable to spoofing resulting either in denial of service or loss of confidence in the reliability of the GPS over large geographical area or specific nodes of the transportation networks. Reliance on GPS leads any user to face a serious threat on the reliability of the service in case of a serious regional or global confrontation.

Example : maritime traffic disruption

Turku's port is a Finnish maritime node of the globalized economy which is dependent on uninterrupted sea transport : « during a typical month, more than 150 ships arrive at the port of Turku delivering or collecting nearly 3.7 million tons of goods (as well as nearly 250 000 passengers). That's 119 000 tons of goods every single day[35]. » Globally « 80 % of the world's trade still goes by the sea. According to the UN Conference on Trade and Development, the 40 largest ports handle 60 % of all the goods shipped around the world[36]. ».

The gain of this trade pattern is the efficiency and low cost of goods handling through ships and ports infrastructure. This was the result of the connectivity of all the actors from the ship's crew to the port staff introduced by the digital global communication infrastructure. As a consequence, « in case of digital disruption, we don't have the ability to revert a plan B using more manual offloading. The world's extreme dependence on shipping and the lack of manual plan B makes ships and ports a strategic target[37]. » If operations at the port of New York, Rotterdam or Los Angeles, « all among the world's 40 largest port were disrupted even for 48 hours, consumers would quickly feel the consequences as shops' supplies of fruit, meat, shoes or gasoline ran dry[38]. ».

Spoofing of satellite signals has previously been reported from the Black Sea, where a number of ships in June 2017 reported anomalies with their GPS positions[39]. The same

[35] (BRAW, 2018) Elisabeth BRAW, (5/11/2018), there's non plan B for port security : privatization and automation have left global shipping fatally exposed, Foreign policy
[36] (BRAW, 2018) Elisabeth BRAW, (5/11/2018), there's non plan B for port security : privatization and automation have left global shipping fatally exposed, Foreign policy
[37] (BRAW, 2018) Elisabeth BRAW, (5/11/2018), there's non plan B for port security : privatization and automation have left global shipping fatally exposed, Foreign policy
[38] (BRAW, 2018) Elisabeth BRAW, (5/11/2018), there's non plan B for port security : privatization and automation have left global shipping fatally exposed, Foreign policy
[39] (NILSEN, 2018) Thomas NILSEN, (2 November 2018), Pilots warned of jamming in Fin mark, The Barents observer

GPS signal malfunction has been reported in Eastern Mediterranean on March 2018 detected by maritime activities[40].

The GPS technological security dilemma

Denial of GPS service or uncertainty on its integrity, over localize or large geographic areas and for extended periods of time is a critical threat for maritime and even air transportation. Following J. Nye and R. Keohane, uncertainty about the liability of the GPS defines an issue area because relationship between fishing, commercial navigation, offshore drilling and military uses are becoming linked functionally for technical reasons and political will[41].

In a case of rivalry between two powers, electronic warfare and spoofing weapon gives a strategic advantage to defection instead of cooperation. Indeed, electronic warfare and cyber weapon are anonymous weapons, and their development is a permanent technological breakthrough following an unpredictable diffusion "S" curve. It is a classical security dilemma[42]. Such capacities are accessible to a lot of countries. As a consequence, any great power will develop fully its capacity to rely solely on its own GPS. The GPS issue area is structured by this security dilemma.

The decrease cost of electronic warfare and the new spoofing cyber weapons diminish the hegemonic position of the US armed forces and the credibility of the US as a keystone of the global security architecture, especially in the case of an hybrid warfare conflict. As a consequence, the rise of the Chinese GPS "Beidou" system is not simply one more positioning service in competition with the US one, it is a strategic challenge.

THE CHINESE BEIDOU CHALLENGE

China will provide a global positioning service in 2020 through its 36 satellites constellation around the earth and the associated Beidou-3 systems, a direct competitor

[40] (US PNT Advisory Board, 2018) US national PNT advisory board, (17 May 2018), GPS Russia undermining confidence in GPS
[41] (NYE, 2001) Joseph NYE, Robert KEOHANE, (1998), Power and interdependence, ed Pearson
[42] or a well known prisoner dilemma in the game theory

of the American GPS[43]. It also uses the 5G network infrastructure, mainly provided by HUAWEI. It is a military and civilian position global service. It is the result of its strategic decision taken in 2000 to become independent from US technologies. It covered East Asia in 2012[44]. Following the *Washington Post*, in 2018, China launched more rockets into space than any other country, some were carrying satellite for the Chinese GPS and China is also pursuing a space power status.

Beidou is used by the Chinese armed forces : the PLA. It brings full autonomy to China in matters of position and navigation services for ground, sea and air transportation means on a global scale. This is the end of its strategic vulnerability from the US GPS, it was developed to end reliance on foreign controlled communication networks. The PLA used Beidou since 2014[45].

The Chinese manufacturers of smartphone, computer, car, ship, plane and public service providers, must integrate Beidou as the default global positioning and tracking services. In the civilian sector, 70 % of smartphone in China are connected to Beidou[46]. In 2018, Beidou provides position for 35 000 public services, 6 million cars, 80 000 buses, 400 commercial ships and aircrafts[47].

It will be the position service for the Belt and Road Initiative and its 120 country members. Around 70 country members (Thaïland, Pakistan, Laos, Brunei, etc.) are already partners and candidates to use this system for navigation services[48]. There are hundreds of ground stations in Thailand to support the Beidou satellites[49]. Today, it is already used by 300 million users spanning 200 countries[50]. It will develop interoperability with the Russian Glonass position service. It is interred operable with the US GPS since 2017.

[43] (PALMER, 2019) James PALMER (August 2019), Decoding China's 280-character web of disinformation, Foreign Policy
[44] (FOUQUET, 2018) Claude FOUQUET, 27 December 2018, Beidou, le GPS chinois commence à fournir ses services au niveau mondial, Les Echos
[45] (SLOANE, 2020) Heath SLOANE, 7/4/2020, Precision politics : china's answer to GPS comes online, The Diplomat
[46] (BAGATINE, 2018) Richard-clément BAGATINE (September 2018), 5 ans après l'annonce des nouvelles routes de la soie : situation et perspective, ASIA FOCUS, n°85
[47] (FOUQUET, 2018) Claude FOUQUET, 27 December 2018, Beidou, le GPS chinois commence à fournir ses services au niveau mondial, Les Echos
[48] (BAGATINE, 2018) Richard-clément BAGATINE (September 2018), 5 ans après l'annonce des nouvelles routes de la soie : situation et perspective, ASIA FOCUS, n°85
[49] (SLOANE, 2020) Heath SLOANE, 7/4/2020, Precision politics : china's answer to GPS comes online, The Diplomat
[50] (SLOANE, 2020) Heath SLOANE, 7/4/2020, Precision politics : china's answer to GPS comes online, The Diplomat

The US GPS provides position service for 3,6 billion receivers among which 3 billion smartphones. Foreign Policy magazine emphasized that Beidou is a two-way communication system. It allows China to identify the locations of receivers and it could be used in cyberattacks.

MITIGATION AND THE FRAGMENTATION ISSUE

Following the National Space-Based Positioning Navigation Timing Advisory Board, an independent body that advises the US government on GPS, in this new context the US GPS system cannot serve as a sole source for position, localization or precision timing for certain critical applications. Utilization of backup systems and procedures in applications where the consequences of losing GPS are unacceptable will ensure optimum safety. Backup for positioning and precision timing are necessary for all GPS application involving the potential for life-threatening situations. The backup option involves some combination of terrestrial or space-based navigation and precision timing systems, on board airline and vessel systems and specific operating procedures.

So, the main mitigation barrier is to use diverse means of navigation with dissimilar security failure modes to GPS[51]. Mitigation by redundant systems, backup systems and contingency systems. The diversity of the components and the architecture and electronic features of each system may be used as a mitigation barrier. Alternative navigation systems, and operational procedures are required to maintain or even increased the diffusion of the position services.

Hence, the main option to reduce GPS service vulnerability is to develop the capacity to switch from one positioning system to another one. Namely, interoperability between navigation information services. This kind of governing and companies arrangement

[51] (GRANT et al., 2009) Alan GRANT, Paul WILLIAMS, Nick WARD, Sally BASKER, (April 2009), GPS Jamming and the impact on maritime navigation, Journal of navigation volum 62 n°2, pp 173-187

between position services providers and users is referred to an international regime : "by creating or accepting mitigation standard of equipment reliability and operational procedures and institution for certain kind of activity, air and maritime activity, government regulate and control transnational and interstate relations[52].".

This interoperability feature may be enforced through international institution like NATO for defence, which enable interoperability among many European and American armed forces systems. However, such international institution has an important necessary condition : who is the security provider ? Indeed, to enable interoperability, one must be sure that any participant will not use the global common, the GPS position service, against another one. The recent buying of Russian ground to air missile S400 by Turkey, which is a NATO member, illustrate such shortage. Indeed, the Turkish S400 system enables Russia to monitor exactly the position of its targets in real time. Like electronic warfare and spoofing provide any country the possibility to use the GPS in case of conflict, it offered any member the capacities to make defection to the cooperation. As a consequence, only one country must be the "owner" of the GPS in order to make sure it may not be used by another member. Hence, an international regime with only one keystone country as the only global security provider is a hub and spoke alliance. An international regime may support interoperability, but it requires a dominant country to settle the agreement in the time duration and provide security for all members. The gain for all the participants is reached under the "shadow of future" that the global common cannot be used as a political lever detrimental to any member. Any international regime required a political structure to produce rules to frame the benefits for each participant of an interdependence. In the case of GPS, it also requires only one security provider which changes the nature of the international regime into an alliance.

[52] (NYE, 1998) Joseph NYE, Robert KEOHANE, (1998), *Power and interdependence*, ed Pearson

Indeed, liberals promote another kind of mitigation for a global common. They tend to neutralize the political lever offered by these technologies, GPS, etc. and to provide a liable positioning service with an international organization.

The GPS service quality, safety and security have a certain cost and to reduce the cost the providers and the users could establish common rules, or international regime, to govern which behaviour is acceptable or not. It is rising the need for an alternative regime where the position services would be a global neutral service. 90 % of international trade uses maritime infrastructures, ships and ports, to move goods from the manufacturers to the customers. The quantity and speed of product flows required interconnexion of vessels and ports to track their position and coordinate resources. Ports assigned a place to embark or discharge containers. A business or a set of businesses through an international organization may provide the required quality level of a positioning service.

However it couldn't guarantee the neutrality of the behaviour of its countries members. Especially in front of the kind of advanced persistent threat offered by the low cost electronic warfare and cyber weapons which rest on social engineering and zero day vulnerabilities to penetrate networks, complete a full reconnaissance and implement, what is needed in case of confrontation or simply to collect data to draw on intelligence for the longest time possible. As a consequence, facing a permanent threat induces by a permanent innovation breakthrough of electronic warfare and cyber weapons and without force at a global level and a permanent possibility of confrontation, the fragmentation of the positioning service becomes a trend. Such strategic environment requires a linkage between the states and businesses, GPS providers and users, that makes a serious impetus for a state strategy. The "loyalty" of the positioning service businesses and the security of its components and systems become the main criteria for any technological solution. Hence, the convergence between electronic warfare and cyber weapon entails to give up the interdependence concept to the benefit of the connectivity concept. However, in contrary to an interdependence, there are no cross dependences between the provider/user of a connection. The only way to securize a connection is to

enable inter operability between severals systems providing the same function, but relying on different technological vulnerabilities. As a consequence, each great power will support its own set of systems through alliances.

TECHNOLOGICAL BREAKTHROUGH AND SHIFTING ALLIANCES

Russia use spoofing GPS technics at frontiers to leverage the field of confrontation[53]. Russia electronic warfare capacities become a real threat to digital devices such as GPS receiver and radios even smart phones. Spoofing technics leure civilian GPS signals and provides the receiver with false coordinates. For example, the spoofing of the GPS signals use by drone transmits airport coordinates to civilian users of drones because commercial drones typically come preprogrammed with safety mechanisms that make them automatically land or shut down when they enter the airspace of an airport[54]. Drones operating near the strategic asset will shut down automatically and land when they come within the range of the spoofer. Hence, the use of spoofing technics is a low-cost tool to provide security within a determine area. However, this use by the Russian in the Black Sea was detected by the automatic identification systems of nearby ships systems that rely in part on GPS. The ships started reporting their locations at the Simferopol Airport about 125 miles away from their actual position or at the Anapa Airport in mainland Russia[55]. During NATO's Trident juncture exercise, held in Norway in 2018, GPS signals failed. Civilian airplanes were forced to navigate manually and ordinary citizens could no longer trust their smartphones. Nine in ten smartphone owners use GPS supported apps[56]. Spoofing technics illustrate the main difference between connectivity and interdependence. One cannot balance its dependence by another cross dependence to develop trust between participants. The vulnerability carried by connectivity required interoperability between systems and a political structure to enforce security between providers and users.

[53] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy
[54] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy
[55] (GROLL, 2019) Elias GROLL, (3 April 2019), Russia is tricking GPS to protect Putin, Foreign Policy
[56] (BRAW, 2018b) Elisabeth BRAW, (17 December 2018b), The GPS wars are here, Foreign Policy

Under the threat of the technological convergence of electronic warfare and cyber weapons connectivity induces interoperability. However, connectivity is not interdependence. Due to dramatic cost decreases, the military electronic and cyber weapons capacities of challenging government like China change the available strategic options offered to other second rank countries. They are no more in a situation where they must accept a detrimental alliance. The consequence of the Beidou position service is the decoupling of countries of their reliance on US GPS and its hub and spoke alliances architecture[57]. The jamming and spoofing vulnerabilities may triggered on the short term an increase in the cost of navigation systems and a spiral of political actions and reactions on the long term. Risk aversion for safety issues and information uncertainty will fuel this spiral. Each actor becomes focus on the transportation risk issues and the level of security requirement may reach an unsustainable level regarding the benefit of globalization. The US GPS capacities of the US hegemon which were a global common and required the survival of the existing hegemonic security architecture is challenged by China and its new Beidou position service. ■

[57] (SLOANE, 2020) Heath SLOANE, 7/4/2020, Precision politics : china's answer to GPS comes online, The Diplomat

ASIA FOCUS #141

THE CHINESE GLOBAL POSITIONING SERVICE AND THE CONVERGENCE BETWEEN ELECTRONIC WARFARE AND CYBER ATTACK

By EMMANUEL MENEUT / Ph.D, Lecturer at the Catholic Universities

MAY 2020

ASIA FOCUS
Collection supervised by Barthélémy COURMONT, research director at IRIS, lecturer at the Université Catholique de Lille, and Emmanuel LINCOT, associate research fellow at IRIS, professor at the Institut Catholique de Paris – UR "Religion, culture and society" (EA 7403) and Sinologist.
courmont@iris-france.org – lincot@iris-france.org

ASIA PROGRAM
Supervised by Barthélémy COURMONT, research director at IRIS, lecturer at the Université Catholique de Lille.
courmont@iris-france.org

THE FRENCH INSTITUTE FOR INTERNATIONAL AND STRATEGIC AFFAIRS
2 bis rue Mercoeur
75011 PARIS / France
T. + 33 (0) 1 53 27 60 60
contact@iris-france.org
@InstitutIRIS
www.iris-france.org