



"We will coup whoever we want. Deal with it."

An appraisal of technology for geopolitical control.

A wolf in sheep's clothing.

SpaceX Starlink

CHAPTER I: THE WORLD WE LIVE IN

1. India's need for sovereignty and technical independence has been artificially held back in the past and present. Is Starlink the latest tool brought upon by U.S.A. to impede India's New Space, Defense & intelligence, and telecom capabilities?
2. With sanctions and restrictions imposed by the U.S.A. every decade, Indian scientific & engineering programs face abnormal hurdles; we ultimately achieve great outcomes despite this forced adversity:
 - A. India's nuclear program: despite Homi Bhabha's assassination, we went on Operation Shakti and became a nuclear deterrent state. [1]
 - B. Rocket engines: despite the cohesive move against India's program, we went on to build one of the most successful Space Programs in the world. [2]
 - C. Fighter Jet: sanctions spread across 3 decades have not been able to hold back the development of the Tejas. [3]
 - D. GPS: denial of GPS in the Kargil war to the Indian Forces by the U.S.A., created a reason for U.S.A. to build the NaVIC constellation. [4]
 - E. Missiles: MTCR (lead by U.S.A.) restricted development of Indian missiles, ultimately leading to indigenous missiles that are now class leading globally, including Agni. [5]
 - F. In more recent years, in 2019, India has another mission also called Shakti, testing an anti-satellite (ASAT) missile. Becoming the 4th nation after U.S.A., Russia & China to test them live and destroy a sat. The USA was strongly against the test. "NASA Administrator Jim Bridenstine touched on testing that creates space debris in a U.S. House of Representatives hearing on NASA's proposed budget on March 27. "Debris ends up being there for a long time. If we wreck space, we're not getting it back," Bridenstine said. "And it's also important to note that creating debris fields intentionally is wrong ... because some people like to test anti-satellite capabilities intentionally and create orbital debris fields that we today are still dealing with. And those same countries come to U.S.A. for space situational awareness because of the debris field that they themselves created.
"And that's being provided by the American taxpayer, not just to them, but to the entire world for free," he added. "The entire world [has to] step up and say, 'If you're going to do this, you're going to pay a consequence.' And right now, the consequence is not being paid." [6]
3. Pre-capitalist forms of domination were based largely on brute military force and, at the local level, on kin networks. Only occasionally, and slowly and unevenly, did pre-capitalist empires build common ethnic or cultural identities, and they did so mainly among elites; even less often did they had any effect on the organization or technical level of production of the territories they conquered. As a result, ancient empires were able to exert hegemony only in the military realm. Their control over the economy of conquered territories, and even of much of their homeland, was far from hegemonic. By contrast, modern forms of dominance have been able to rapidly and decisively transform the territories and people that they controlled. [7]
4. As the Empire of the world, the USA has the task of defending its position, and to do that it must not only strengthen itself but also weaken others. The strategies that states put in place to increase their economic power and their impact on the international balance of power can be interpreted only by the concept of

economic warfare. [8] The mechanism of control has changed, these strategies and mechanisms are more subtly engineered. With the four levers for control being:

- Media /Social Media Narratives & Entertainment
- Intelligence – Signals, Systems, Humans, Geospatial etc.
- Military / Arms
- Financial Institutions and Currencies

5. An Empire has no friends, it has subjects, even the ones favoured will still be sacrificed for the needs of maintaining the power status quo. The examples below illustrate known American economic warfare against even their closest NATO allies.

Examples of economic warfare by the U.S.A. Govt for American enterprises:

- A. United States intelligence agencies have not only targeted Chancellor Angela Merkel's cell phone, but they have also used the American Embassy in Berlin as a listening station. The revelations now pose a serious threat to German-American relations. Research by SPIEGEL reporters in Berlin and Washington, talks with intelligence officials and the evaluation of internal documents of the U.S.A.' National Security Agency and other information, most of which comes from the archive of former NSA contractor Edward Snowden, lead to the conclusion that the U.S.A. diplomatic mission in the German capital has not merely been promoting German-American friendship. On the contrary, it is a nest of espionage. From the roof of the embassy, a special unit of the CIA and NSA can apparently monitor a large part of cell phone communication in the government quarter. And there is evidence that agents based at Pariser Platz recently targeted the cellphone that Merkel uses the most. ***"Spying between friends, that's just not done," said Merkel*** on Thursday at a European Union summit in Brussels. "Now trust has to be rebuilt." But until recently it sounded as if the government had faith in its ally's intelligence agencies. [9]
- B. In the early 1990s, the U.S.A. National Security Agency intercepted the communications between the European aerospace company Airbus and the Saudi Arabian national airline. In 1994, Airbus lost a \$6 billion contract with Saudi Arabia after the NSA, acting as a whistleblower, reported that Airbus officials had been bribing Saudi officials to secure the contract. As a result, the American aerospace company McDonnell Douglas (now part of Boeing) won the multibillion-dollar contract instead of Airbus. [10]
- C. The United States defense contractor Raytheon won a U.S.A.\$1.3 billion contract with the Government of Brazil to monitor the Amazon rainforest after the U.S.A. Central Intelligence Agency (CIA), acting as a whistleblower, reported that Raytheon's French competitor Thomson-Alcatel had been paying bribes to get the contract. [11]
- D. In order to boost the United States position in trade negotiations with the then Japanese Trade Minister Ryutaro Hashimoto, in 1995 the CIA eavesdropped on the conversations between Japanese bureaucrats and executives of car manufacturers Toyota and Nissan. [12]
- E. In 1999, Enercon, a German company and leading manufacturer of wind energy equipment, developed a breakthrough generator for wind turbines. After applying for a U.S.A. patent, it had learned that Kenetech, an American rival, had submitted an almost identical patent application shortly before. By the statement of a former NSA employee, it was later claimed that the NSA had secretly intercepted and monitored Enercon's data communications and conference calls and passed information regarding the new generator to Kenetech. However, later German media reports contradicted this story, as it was revealed that the

American patent in question was filed three years before the alleged wiretapping was said to have taken place. As German intelligence services are forbidden from engaging in industrial or economic espionage, German companies have complained that this leaves them defenseless against industrial espionage from the United States or Russia. [13]

- F. According to Wolfgang Hoffmann, a former manager at Bayer, German intelligence services know which companies are being targeted by U.S.A. intelligence agencies but refuse to inform the companies involved. [14]

6. These acts of espionage, economic warfare, and control are legal for the U.S.A., and extra judicially across the entirety of the world. It is legitimized via the following publicly known regulatory framework:

A. Corporate – Economic Espionage Act of 1996

- i. The Economic Espionage Act of 1996 (Pub. L. 104–294, 110 Stat. 3488, enacted October 11, 1996) a 6 titles extraterritorial jurisdiction Act of Congress deals with a wide range of issues, including not only industrial espionage (e.g., the theft or misappropriation of a trade secret and the National Information Infrastructure Protection Act), also requirements for presentence investigation reports, and the United States Sentencing Commission reports regarding encryption or scrambling technology, and other technical and minor amendments. [15]
- ii. Provisions do not apply to activity by government entities, or to the reporting of any suspected violation of law to any such entity. [16]
- iii. In 2000, the European Parliament voted to carry out an investigation into the international surveillance project ECHELON. That same year the French government also began an official investigation into allegations that several collaborating nations may be using the program for illegal purposes. U.S. Central Intelligence Agency documents had been revealed to the British press, showing that the U.S. has been using the technology to monitor European business communications. The French and European allegations centered on the suspicion that such information was being passed to U.S. firms. The U.S. stated that monitoring was focused on the participation of European firms in supplying foreign WMD (weapons of mass destruction) programs, such as the Iran nuclear program, on evading sanctions in Iran and Libya, and on the bribery of foreign officials, such as French payments to Saudi Defense officials. [17]

B. Foreign entities – FISA (Foreign Intelligence Surveillance Act)

- i. Enacted in 1978, FISA establishes procedures for the surveillance and collection of foreign intelligence information, allows the government to conduct electronic surveillance and physical searches for foreign intelligence purposes, subject to approval by the Foreign Intelligence Surveillance Court (FISC) USA. [18]
- ii. FISA enables the collection of foreign intelligence information, particularly regarding non-U.S. persons. It allows for warrantless surveillance and has faced criticism internationally for its lack of transparency and abuse of power. [19]

C. Individuals across the world – CLOUD Act

- i. The Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in March 2018, represents a significant shift in how the United States approaches the collection and access of digital information stored outside its borders. In an increasingly interconnected world, where data is frequently stored in various locations across the globe, the CLOUD Act provides the legal framework under which U.S. law enforcement, defense, and intelligence agencies can access data held by American companies, regardless of the data's physical location. [20]
- ii. The CLOUD Act allows U.S. law enforcement agencies to compel U.S. Companies to produce data stored overseas if it pertains to ongoing investigations. This provision has raised significant concerns regarding the potential overreach of U.S. laws into other jurisdictions and the implications for privacy rights of individuals. [21]

D. USA Patriot Act

- i. Enacted in response to the September 11 attacks, the PATRIOT Act expanded the government's surveillance capabilities, allowing for greater monitoring of communications and financial transactions. [22]
- ii. Includes provisions for roving wiretaps, access to business records, and enhanced information sharing among government agencies. [23]
- iii. Enacted in the wake of the September 11 attacks, the USA PATRIOT Act significantly expanded the surveillance powers of U.S. intelligence agencies. It authorized the FBI and NSA to conduct wiretaps, monitor emails, and access financial records without a warrant, aiming to enhance national security. [24]

E. United Kingdom – United States of America Agreement (5 Eyes)

- i. A multilateral agreement for cooperation in signals intelligence between Australia, Canada, New Zealand, the United Kingdom, and the United States. The alliance of intelligence operations is also known as the Five Eyes. These allied countries include NATO members, other European countries such as Sweden. [25]
- ii. During the 2013 NSA leaks Internet spying scandal, the surveillance agencies of the "Five Eyes" have been accused of intentionally spying on one another's citizens and willingly sharing the collected information with each other, allegedly circumventing laws preventing each agency from spying on its own citizens. [26]
- iii. NSA has a "massive body" called the Foreign Affairs Directorate that is responsible for partnering with other Western allies such as Israel. [27]

Referring to Five Eyes, former French President François Hollande has said that his country is *"not within that framework and we don't intend to join."* According to a former top U.S.A. official, *"Germany joining would be a possibility, but not France – France itself spies on the U.S.A. far too aggressively for that."* [28]

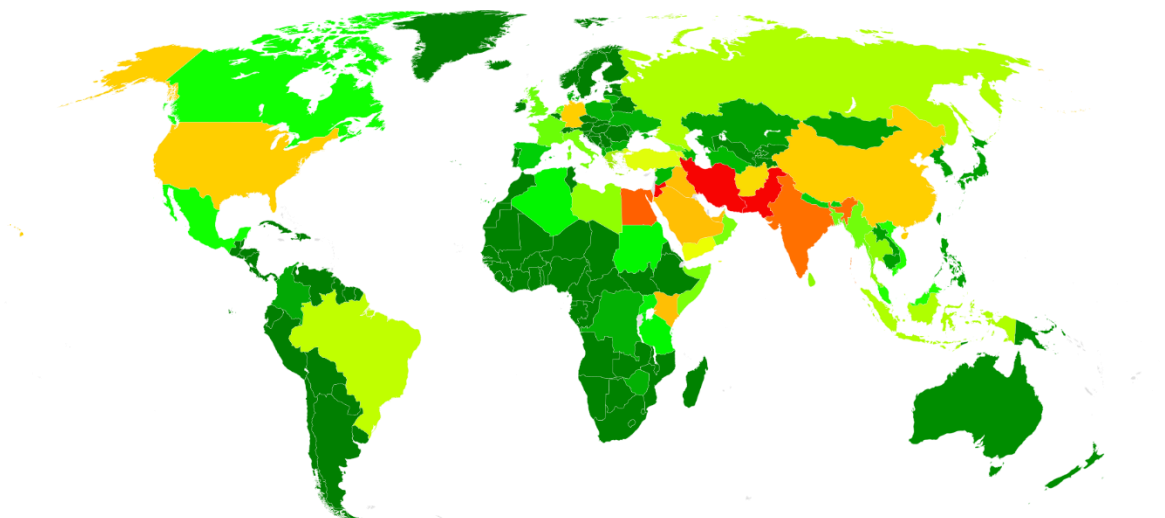
- 7. Under the laws mentioned in point 6, in effect, the U.S.A. Govt & it's agencies whether Govt or private have a possibility, rather a duty as a good patriot to make sure to run programs that deepen American economic

and military hegemony across the world. This can be seen by the various programs running of govt and private enterprises in the following table, marked with which intelligence programs Starlink enables:

#	Program	Program Objective	Data Collected	Purpose	Platform
1	PRISM [29]	Collects data from tech companies targeting foreign nationals, sometimes capturing U.S. data	Emails, chats, videos, stored data	Foreign intelligence and counterterrorism	Starlink
2	XKeyscore + PINWALE + TRAFFICTHIEF [30]	Allows real-time access to global internet data for analysis	Emails, online chats, browsing histories	Enables rapid intelligence analysis	Starlink
3	Upstream Collection [31]	Intercepts communications from fiber-optic/equivalent cables in real-time	Voice, video, text	Captures global communications for intelligence	Starlink
4	Boundless Informant [32]	Visualizes and analyzes data collected globally by the NSA	Metadata from various sources	Provides metrics on NSA's data collection	
5	MYSTIC [33]	Intercepts and archives global voice communications	Phone call metadata, voice content	Foreign voice intelligence collection	Starlink
6	TURBINE [34]	Automates data collection from multiple sources	Data from multiple sources	Streamlines NSA data collection	
7	FAIRVIEW [35]	Collects data from foreign users through telecom partnerships	Voice, text, internet data	Foreign intelligence via telecoms	Starlink
8	BULLRUN [36]	Circumvents encryption to access secured communications	Encrypted communications	Collects intelligence despite encryption	Starlink
9	STONEGHOST [37]	Network operated to carry and share all data across 5 Eyes	Military, SIGINT, foreign intelligence	5 Eyes network	Starlink
10	INTELINK [38]	Secures classified data sharing across U.S. intelligence agencies	Classified intelligence data	Facilitates inter-agency communication	Starlink
11	SOMALGET [39]	Collects voice and data from foreign countries	Voice data, metadata	Monitors foreign adversaries	Starlink
12	Room 641A [40]	AT&T facility for NSA's data interception activities	Internet and telecom data	Provides NSA with direct surveillance	
13	ECHELON [41]	International signals intelligence network with global partners	Phone calls, emails, satellite data	Intercepts global communications for security	Starlink
14	MINARET [42]	Monitors targeted individuals and groups' communications	Targeted communications	Detects potential terrorist activities	
15	GEOINT Programs [43]	human activity by analysis of geospatial information	imagery & geospatial data	Describes, asses, analyse, exploit	Starlink
16	SIGINT/COMINT/ELINT Programs [44]	Intercepts electronic communications globally	Voice, data, communications	Monitors foreign threats	Starlink
17	Chatter [45]	Analyzes communication patterns for threat detection	Online communication, social media data	Assesses potential threats	
18	DROPMIRE [46]	Aimed at surveillance of foreign embassies and diplomatic staff, including NATO allies	All the diplomatic cables	Analyzes and shares intelligence	Starlink
19	TURBULENCE [47]	Offensive cyberwarfare capabilities, like injecting malware	Industrial, military, remote, and infrastructure	Record, analyze, and inject data	Starlink
20	STATEROOM [48]	interception of international radio, telecommunications and Internet traffic.	ALL DATA	Information Sharing, including Five Eyes (Canada) + Israel	Starlink

8. Existing impact on India just with the ECHELON, STATEROOM, and Five Eyes program:

The aforementioned programs have a deep impact already on India, as India is already a major intelligence target, the following map published by the NSA is a testament to the fact that we are amongst the highest data extracted countries in the world for NSA:



Map of global NSA data collection, with countries subject to the most data collection shown in red [49]

The whistle-blower Edward Snowden revealed India already has active sites for ECHELON program as under:

Operated by the United States		
Location	Operator(s)	Codename
New Delhi	CIA	SCS

[50]

CHAPTER II: STARLINK, A WOLF IN SHEEP'S CLOTHING

The Starlink constellation of satellites is a new form of Internet Service Providers across the world, unbound by geographic demarcations and natural boundaries. A direct access to every citizen in the world, with no governance structure in between the user and the American one. The following has been proven for Starlink:

- **Dual Use Abuse: An American military and intelligence tool**
- **Disregard for sovereignty & democracy of other nations**
- **Impedes India's Technological Sovereignty**
- The aforementioned are expounded below

1. **Dual Use Abuse:** An American military and intelligence tool Starlink is a Dual Use technology that pushes its own narrative and purpose to be an altruistic one, as a provider of internet for the underserved populations and regions, however it's biggest customer & promoter is the American Government Intelligence and Military.

- A. **SpaceX President Gwynne Shotwell: “We would launch a weapon to defend the U.S.”** [51] The U.S. Congressional Research Service reports **that future satellites in Starshield's participating SDA program may wield interceptor missiles, hypersonic projectiles, or directed energy weapons**, [52] with the program's founder adding *“since Reagan’s day, technology has advanced enough that putting both sensors and shooters in space is not only possible but relatively easy.”* According to SDA Director Derek Tournear, later satellites will take on the *“extremely difficult”* task of maintaining contact with missiles in flight. [53]
- B. **“When I’m never sure what I can say in a public forum, I tend to zip it. But I can say that there is very good collaboration between the intelligence community and SpaceX,” Gwynne Shotwell SpaceX President.** [54] SpaceX forges tighter links with U.S. Spy and military agencies; The Company has grown from a for-hire rocket launcher into a major American-security contractor. The U.S. Defense & Intelligence played a catalytic role in the development of the Starlink program, whether it was sponsoring SpaceX to expand the application scenarios of the Starlink program to the military at the early stage of its launch, or continuously carrying out technical verification tests during the network construction, which fully proved the ability of the Starlink program beyond civilian applications.

C. Intelligence & defense contracts of Starlink:

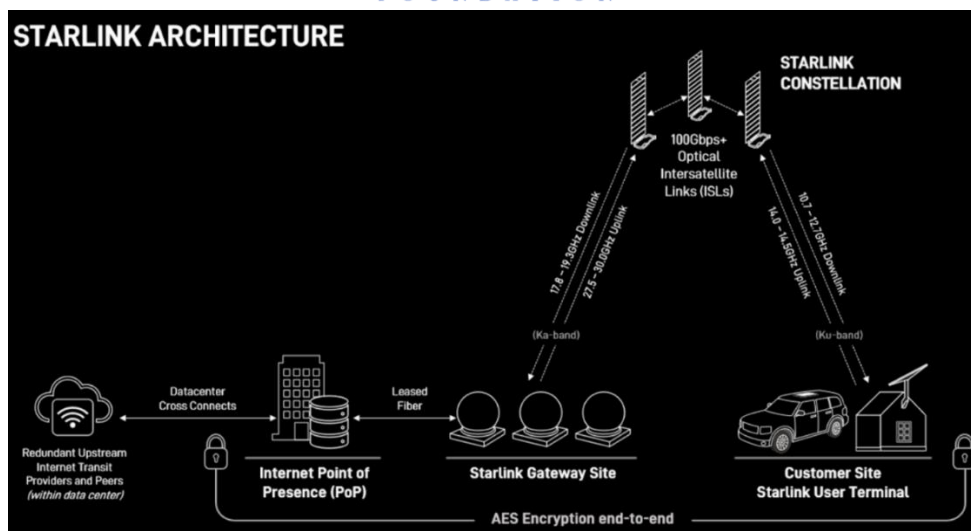
- i. Although SpaceX itself has deep relations with U.S.A.’s defence and military, since their first launch was a customer from the American Defence Forces, Starlink’s intelligence customers trace back to Swarm Technologies which SpaceX bought in 2021, the company was founded with InQtel, the venture capital front of CIA, as an early investor. [55]
- ii. *“The task order for Starshield services is provided by the Starlink satellite constellation but is differentiated from the commercial Starlink service based on unique Department of Defense terms and conditions that are not found in commercial service contracts,”* spokesperson Pentagon. \$70 million contract is a task order under an indefinite delivery/indefinite quantity (IDIQ) procurement vehicle for proliferated low Earth orbit (PLEO) satellite services **“Starshield end-to-end service via the Starlink constellation, user terminals, ancillary equipment, network management and other related services.”** [56] The contract has a \$70 million ceiling, with \$15 million being obligated to the company by the end of this month, Elon Musk wrote that *“Starshield will be owned by the U.S.A. government and controlled by DoD [Department of Defence] Space Force.”* [57]
- iii. **SpaceX has had a classified contract with the U.S.A. National Reconnaissance Office (NRO) since 2021 to build a network of “hundreds” of spy satellites for the agency;** while an NRO spokesperson reportedly declined to comment on Reuters findings about SpaceX’s involvement, it confirmed to the outlet that it’s working to develop *“the most capable, diverse, and resilient space-based intelligence, surveillance, and reconnaissance system the world has ever seen.”* [58]

- iv. In October 2020, SDA awarded SpaceX an initial \$150 million dual-use contract to develop 4 satellites to detect and track ballistic and hypersonic missiles. The first batch of satellites were originally scheduled to launch September 2022 to form part of the Tracking Layer Tranche 0 of the Space Force's National Defense Space Architecture. The launch was rescheduled multiple times, but it eventually launched in April 2023. [59]
- v. These are just the known contracts of Starlink as a part of the Intel-Military-Industrial complex of the USA, there are a lot of confidential agreements and contracts kept behind covers.
- vi. In addition, it is well known that the owner of Starlink, Elon Musk, is close to various private intelligence companies, and is a highly political exposed person in the U.S.A. including but not limited to Palantir Technologies USA, and the Trump Election 2024.



Elon Musk with (now retired, and COO at SpaceX) four-star general Terrence J. O'Shaughnessy in April 2019 [60]

- D.** Space warfare, the next frontier; how Starlink is a dual use technology for warfare and control. A wolf in sheep's clothing, Starlink is a dual use technology player that provides the following use cases currently:



Starlink Architecture [61] showing ground infrastructure radar deployment across Host Nations, 15 out of 20 intelligence aforementioned intelligence programs of CIA/NSA are enabled this architecture

“Starlink antennas use an internally developed, electronically steered phased array tight beam that is more advanced than the best military technology” Elon Musk Tweet on August 26, 2023 [62];

i. **Signals - information intelligence & interception**

The Starlink program provides low-cost, low-latency, high-throughput, and global coverage high-speed Internet services that can significantly enhance the U.S. military’s operational communications capabilities. On the one hand, it can provide more stable and reliable communication capabilities for U.S. military combat units deployed around the world, and on the other hand, it also has the potential to provide high-definition pictures and even live video. Currently, the U.S. has conducted tests using the C-12 military reconnaissance aircraft and achieved a network speed of 610 Mb/s, 102 times the current U.S. military theatre minimum transmission rate requirement of 5 Mb/s. In addition, the U.S. Army has conducted AC-130 helicopter gunship access tests and Army combat platform communications tests and has connected a variety of air and ground military equipment at high speeds via Starlink satellites during live fire exercises. In the near future, the U.S. will be able to use the Starlink program to further enhance the information acquisition capability and speed of the main combat equipment, the F-35 fighter aircraft, while more rapidly transmitting information to other command and control nodes to enhance local battlefield C4 ISR capabilities. [63]

The images below show an Echelon site with the radar technologies of 80s used to intercept signals, gather intelligence, and provide ground control for American intelligence agencies and also a typical Starlink Ground Station/Gateway. The Starlink is more advanced technology of 2020s thus improving an order of magnitude over 4-decade old technology. Additionally, Starlink Ground Station / Gateway sites are installed in multiple numbers across the Host nation (e.g. Brazil has ~16+) [64]



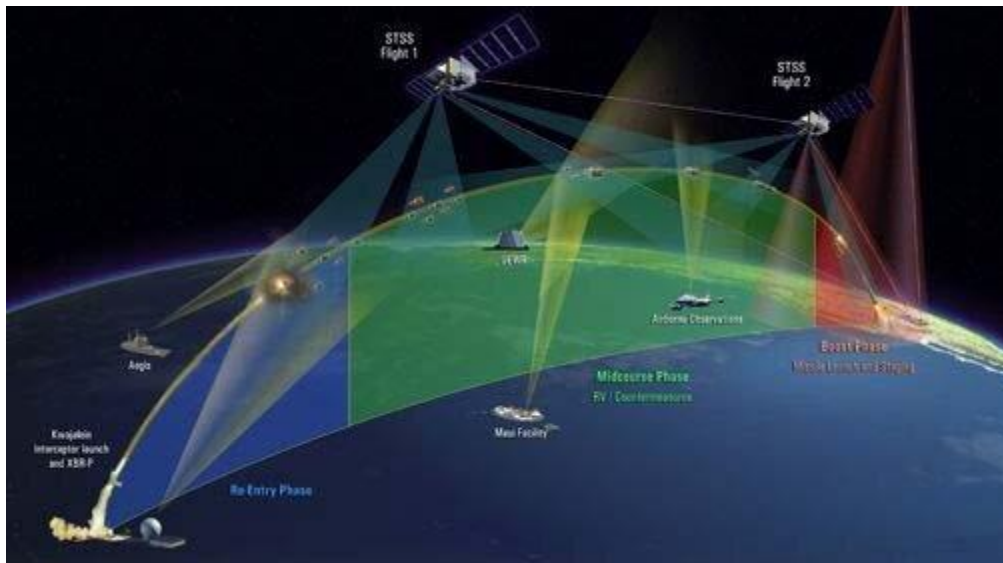
ECHELON site at [RAF Menwith Hill](#), England



Starlink ground station near Usingen, Germany

ii. **All-Weather Earth Surveillance and Reconnaissance Capability**

Starlink has global coverage capability and high revisit rate, especially for the densely populated areas of the world, where several satellites transit the zenith at each moment. By carrying visible, infrared, radar and passive payloads on the satellite, 24-hour continuous surveillance and reconnaissance can be achieved to enhance the surveillance capability of moving targets. [65]



Distributed Space Based Surveillance System monitoring Space, Sky, Land, & sea

iii. **Space-based target detection/suppression capability**

By carrying various sensors, the satellite chain can detect and track satellites, rockets, space debris, missiles and other targets, and support target positioning, orbit determination and orbit prediction. Currently, in order to consolidate and strengthen its space dominance, the United States has proposed a 7-layer next-generation defense space architecture, which aims to build a proliferating low Earth orbit space architecture and unify and integrate the next-generation space capabilities of the U.S. Department of Defense. The U.S. Department of Defense Space Development Agency has commissioned SpaceX to build four anti-missile tracking satellites based on the Starlink satellite platform for its next-generation defense space architecture (national defense space architecture, NDSA) tracking layer to further enhance the missile defense and hypersonic vehicle detection, tracking and indication capabilities. In addition, the

satellite chain has a strong manoeuvring capability to change orbit and can carry robotic arm and other on-orbit operation devices to achieve the approach and disposal of space-based targets. [66]

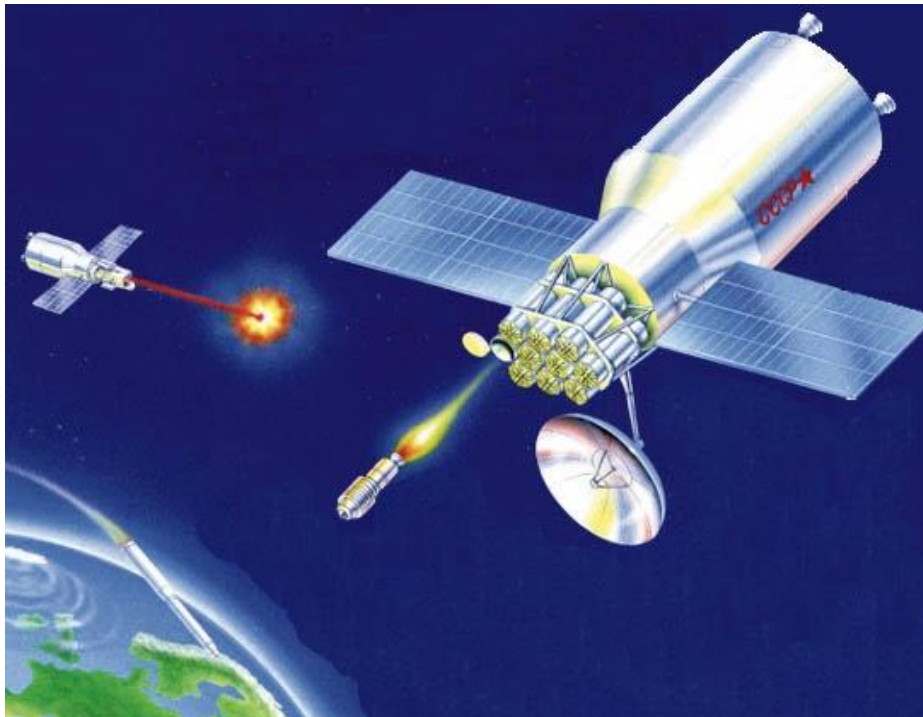


Starlink Ground Station, Fairbanks Alaska USA (800kms from Russia; Satellites sky radar + Ground based Radomes easily enable target detection of even stealth targets

iv. Future combat concept test bed

The United States in the next generation of military satellite system planning to use more constellations based on small satellites to improve the flexibility of space-based systems, anti-destructive capabilities. Starlink satellites can be used as a platform to carry information support payloads such as sensors and communication equipment, greatly enhancing flexibility and anti-destructive capabilities.

At the same time, with the ability to go hand in hand is the ability of the Starlink program to become a vehicle for emerging U.S. warfare concepts, typically represented by mosaic warfare. This new type of combat by arbitrarily combining with standardized functional units, at the functional level to integrate a larger number of smaller, single-function combat elements into more unmanned, autonomous systems to build a kill network with good adaptivity and flexibility, which can be adjusted in a timely manner according to changes in the battlefield posture force structure layout, change the operation of the battle plan, so as to play the maximum effectiveness in the right place, and ultimately confuse the enemy's combat targets, cause "battlefield fog", and gain the dominant advantage in system confrontation. [67]



A United States Air Force illustration of a hypothetical Soviet Armed Forces space weapon [68]

2. Disregard for sovereignty & democracy of other nations

The following evidence are the exemplification of the dangers of Starlink for non-USA nations/states; it is not a judgement on the morality of the issues. The crux of the argument as seen from the following examples is the whimsical public opinion driven decision making that reinforces the control of the U.S.A. Government and intelligence agencies for the decision making other Nations/states; thus, deepening their globalist agenda further.

These examples underscore the role of Starlink as a tool of Geopolitical Control, despite the narratives of being altruist.

- A. **Brazil** – Extract from media that summarizes the issue: *“Elon Musk is doubling down on his fight with the Brazilian authorities; after Brazil's Supreme Court ordered X blocked in the country, he suggested that Brazilians use software to circumvent the ban, despite the risk of large fines that a judge has threatened to impose for doing so. Now he is defying the Brazilian government again. Starlink told the country's telecom agency on Sunday that it would not comply with orders to block X,”* the agency's president said. [69]
- B. **Ukraine** – Starlink has since February 2022 been used by Ukrainian civilians, government and military. The satellite service has served for humanitarian purposes, as well as defense and attacks on Russian positions. Initially, SpaceX provided and funded Starlink services to Ukraine largely on their own. As of June 2023 Starlink expenses for Ukraine are covered by the U.S.A. Department of Defense through a contract with SpaceX. SpaceX executives have declined to extend Starlink availability to Russian-occupied territories of Ukraine like Crimea. This was criticized by Ukraine as it prevented them from carrying out military operations in those areas. Despite this, Starlink is considered to have become a reliable partner to Ukraine in the war, and has become a substitute for modern encrypted real-time communication in warfare. Those **Ukrainians involved in bringing Starlink to their country "originally overlooked**

the significance of [Elon Musk's] personal control" over vital communications. Starlink was first requested during the Battle of Kyiv in early 2022. Starlink is free for the Ukrainian military, and since its activation, Starlink has been used to carry out military operations in Ukraine and is still in use on all front lines as of late 2023. **Starlink legal documents claim it is not for use in weaponry as a military use of Starlink brings it under U.S.A. export control laws like the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). A Ukrainian military official called Starlink's statements "strange" given that the use of Starlink as a combat tool is well-established. [70]**

- C. Gaza – Connectivity denied by Starlink on the behest of Israel.** Showing the influence of a third state can and will have an impact on the connectivity infrastructure of the primary users. Starlink has been inconsistent in his approach toward various governments driven by American intelligence and defense agendas and not international regulation and treaties. After Israel cut all communications in Gaza during its war with the Palestinian Hamas movement on Oct. 27, Elon Musk vowed that *Starlink “will support connectivity to internationally recognized aid organizations”* in the besieged coastal strip. Israel promptly pledged to “use all means at its disposal to fight” the SpaceX owner’s decision, arguing that Hamas would use Starlink’s services “for terrorist activities.” In response, Elon Musk said his company would take “extraordinary measures” to ensure Starlink’s services are “only” used for humanitarian purposes. He added that the firm will also do a “*security check with both the U.S.A. and Israeli governments before turning on even a single terminal.*” [71]
- D. Iran –** Contrary to Gaza, despite the Government’s clear instructions for “*Cessation of Emissions*”, i.e. to stop all connectivity as an unlicensed communication provider in the Republic of Iran, which falls under global regulations of ITU; the connectivity has continued unfettered by Starlink. The ITU — the closest thing there is to a global regulator of communications — ruled in favor of Iran in October and again this month at a meeting of its Radio Regulations Board in Geneva. There, the board dismissed an assertion from the U.S.A. that an operator shouldn’t be expected to verify the location of every terminal connecting to its satellites. The board on March 12 called on the U.S.A. and Norway (which share responsibility for Starlink’s ITU registration) to take “*immediate action*” to disable terminals in Iran. The decision puts the U.S.A. in an awkward position, given the Biden administration’s past encouragement of Starlink use as a means of thwarting Iranian efforts to restrict internet access. In 2022, the Treasury Department eased some restrictions on Starlink in Iran amid widespread protests over the fate of 22-year-old Mahsa Amini, who died in custody after she was arrested for allegedly flouting Islamic dress codes. The U.S.A. acted “**to advance Internet freedom and the free flow of information for the Iranian people,**” Secretary of State Antony Blinken said. In response **Elon Musk on Oct. 28 posted an image on Twitter that showed a map of the region with Iran surrounded by dozens of U.S.A. bases. The text in the image read: “Iran wants war; look how close they put their country to our military bases.” [72]**

3. Impedes India's Technological Sovereignty



- A. Satellite companies have 3 major streams of revenue – Earth Observation & sensor deployment, Communication -data & Location services, defence services.
- B. Starlink plays in all the above 3 fields as a vertically integrated player, and as the largest and most deeply entrenched player in the world, it directly impedes investment into other companies. No investor will invest into the above if Starlink operates in their geography.
- C. Launch providers require payloads to be of value, today SpaceX has a monopoly on the launch market in the world, even taking away launches from ISRO/Antrix/NSIL. This launch cadence is helped as they are cross discounting their own launches of Starlink and maintain a regular schedule for the same, reaching 144 launches in 2024. [73]
- D. Ecosystem Death Spiral:
 - i. Payloads for space launches in each geography reduce because no one will invest in the payloads mentioned above as Earth Observation / Communication / Civil / Defence.
 - ii. Therefore, the requirement to create and operate launch systems / rockets /vehicles reduces significantly.

- iii. Therefore, it makes New Space a very unattractive sector, as a major American defense contractor with the leading technology is a direct competitor to any Space company in the world whether a launch provider or a payload provider.
- E.** The Ecosystem Death Spiral ultimately leads to two potential paths:
- i. Government funded space sector kept alive for only certain missions, missions that over a period become less attractive overtime as the technology gap increases;
 - ii. The second path is to give up, and the whole strategic ecosystem is lost, this is the route that Europe has taken, and its effect is seen on its major industrial player in space: Airbus; In October 2024 Airbus laid off 2500 people from their satellite & space division, for the precise reasons mentioned above [74]
- F.** Whichever path is chosen, the technological gap increases and creates a lack of capacity for Space, and thus cede the industry, technology, and sovereignty, and give into the globalist agenda of U.S.A the Empire, and give up fully on the next frontier of warfare.

CHAPTER III: EVERYTHING TO LOSE, EVERYTHING TO WIN; TAKING A LOOK OUTWARDS AND INWARDS

1. Taiwan

- A. Is heavily partnered with the U.S.A. for its defense programs
- B. Is in a vulnerable position of utmost urgency
- C. hosts a large Starlink supplier base.

Despite the aforementioned 3 critical reasons that would make Taiwan a natural host of Starlink, Taiwan has refused to grant Starlink an ISP license. They require 51% ownership to be local and are now creating their own ecosystem to ensure sovereignty. This is despite them lacking a space program and a space ecosystem; this national resolve for sovereignty and their understanding of leading-edge technology makes them take the path of independence and Atmanirbharta. [75]

2. China

A Space giant, China is creating their own mega-constellation which has already kickstarted a large ecosystem of New Space and satellite companies in the country. China has a resolve for creating a space force which will be leading in the world, as a matter of policy they understand that Space is next frontier of warfare, economic and military. [76]

3. Russia

The Old Space leader, Russia is building their space warfare and New Space capabilities in the face of economic sanctions. With a deep understanding of space and its importance, with the honour of also being

one of the first creators of concepts of constellations Russia is well placed with a deep technical expertise, with a national level focus on building the ecosystem for Space warfare. [77]

4. India

- A.** India has the ingredients that has lead to a flourishing ecosystem, and even lead the world in true democratic access to Space.
- i. A mature and world class space program [78]
 - ii. World class telecom providers supporting 1.2 billion users already [79]
 - iii. Large cohort of New Space companies ready with technology [80]
 - iv. Large consumer base – agriculture, forestry, risk management, urban development, disaster management, shipping, aviation, mining, resource management, oil & gas, road infrastructure, energy infrastructure, defence, security & intelligence, meteorological department, underserved communities, railways, etc. [81]
 - v. Large investor base – with already ~1 billion USD invested in the field of New Space across startups, PSUs (NSIL/Antrix/ISRO/DRDO/HAL), and large corporates (Godrej/TATA/Mahindra/L&T). [82]
- B.** Legal and Geopolitical Framework Considerations for Foreign Involvement in this sensitive technology: India has enacted several laws and regulations that safeguard national security and data integrity. These legal frameworks govern foreign investment, data protection, and the operation of technology companies in the country.
- i. The Information Technology Act, 2000: This act regulates cyber activities and provides a framework for data protection and cybersecurity. It empowers the government to impose restrictions on foreign entities that pose a threat to national security. [83]
 - ii. The National Cyber Security Policy: The policy outlines India's approach to cybersecurity and emphasizes the importance of protecting critical infrastructure from foreign threats. It recognizes the need to assess the security risks associated with foreign ISPs and technology providers. [84]
 - iii. WTO Regulations: International norms and standards emphasize the importance of national security in procurement processes. The World Trade Organization (WTO) encourages member nations to prioritize national security in procurement, allowing for restrictions on foreign entities in sensitive sectors. [85]
 - iv. **ITU: Radio and telecommunication** are critical national resources; Article 34, Article 35, Radio Regulations Article 18, Resolves 1 & 2 of Resolution 22 (WRC-19), & the resolves of Resolution 25 (WRC-03), & others; make it very clear that the ITU Constitution recognizes the sovereign right of each Member State to regulate its telecommunications in any manner it deems fit; and terminate any service especially if it poses a security challenge.
- C.** Reaping the rewards
- 1.2 billion people are connected in India via cellular networks, that leaves 0.2 billion disconnected, even if 10% of that is the market serviced by India's constellation (i.e. 20 million), at 50% current data prices of Starlink; that means 20 million people served with an annual subscription fee of Rs. 72000 / USD 840; the

revenue potential translates to 17 billion USD/ Rs. 1.44 Lakh Crore per year. Or 85 billion USD / Rs. 7.2 Lakh Crore in 5 years.

- i. If this price doesn't work for "underserved communities" for internet access, then there is no market for Starlink anyway, which means that there is no point in their projected motive.
- ii. However, if we believe that this price will work, and create real social change; social change that PM Modi's India has repeatedly delivered upon, especially by connecting a billion + people in the last 5 years to high-speed mobile internet;
in that case the revenue stream should be used as a multiplier for Atmanirbhar Bharat.
- iii. All of this revenue will commercialize the technological capabilities that are already present in India; along with massive sovereignty advantages and large export potential, upwards of 150 billion USD in the next 5 years, for Indian Earth Observation and communication companies.
Thus creating a net positive inflow, not a net negative outflow.

D. Risks mitigated by Atmanirbhar Bharat

- i. As Satcom technology goes into its third generation, i.e. to Direct to Cell; Starlink will threaten Reliance Jio, BSNL, and Airtel; [86]
- ii. Our New Space industry story will be stymied significantly with weakened investor, creator, and entrepreneurial interest.
- iii. India's security and intelligence will be beholden to American interests. As it is being seen by even their NATO allies. [87]

CHAPTER IV: CONCLUSION

1. Looking back at the three levers of control for a hegemon in light of Starlink:
 - A. Media /Social Media Narratives – Providing internet to the underserved regions provides the required legitimacy of the narrative and system of the U.S.A. and Starlink bringing freedom and access to remote corners of the world.
 - B. Intelligence – Signals, Systems, Humans, etc. – Starlink has Space based sensor mesh and Ground Stations with advanced radars directly connected to core internet infrastructure of a host nation, while being in the extraterritorial jurisdiction of the USA due to space-based sensors and immutable communication.
 - C. Military / Arms – Largest customers being defence agencies of the USA with open declarations by owners and management of Starlink, with real practical examples of using Starlink in warfare and to wield American political will in extra judicial territories without recourse.

Thus, Starlink is (very candidly) a technology of geopolitical control, pushed by intelligence and defence forces to have the dominance in space and control over land via that lever.

2. In effect the threat is not only Starlink, but also other American, Chinese, Russian, etc. with a host of Mega constellations coming online, India must build countermeasures, with the following immediate requirements:
 - A. Mega Constellation wide area surveillance capability
 - B. Precise sensing of key targets
 - C. Capability for comprehensive intelligent fusion of situational data
 - D. Capability to recover from anomalous events in outer space.
 - E. Low orbit group target system countermeasure capability
 - F. And of course, to build out our own mega constellation as one of the most powerful nations in the world.

3. Therefore, protectionism is a legal and pragmatic approach in face of a technological paradigm shift is not just against Starlink as an individual entity, but in protection of India's Space and Security future from the **concerted efforts of the American and other nations' Intelligence Agencies, Defense Complex, and Extra Territorial Judicial systems, that Starlink represents.**

Satellite ownership is important for economic growth and national security. Ownership ensures operational independence, privacy, and priority in the security of the country.

With no Lok Sabha elections in the coming 4 years, the Modi Government has just enough time to take the measures to secure India's future and bring to life our Mega Constellation before 2029.

Sources

- 1 Kumar, P. (2024). Homi J. Bhabha: A Complete Biography: Homi J. Bhabha: A Complete Biography: Architect of India's Nuclear Program. Prabhakhar Prakashan Private Limited. p. 1960. ISBN 978-93-5562-
- 2 ISRO spy case: SC judgment will help to change mindset of law enforcement machinery, says Nambi Narayanan". Firstpost. 14 September 2018. Retrieved 25 August 2023.
- 3 <https://sputniknews.in/20240818/is-us-delaying-supplies-of-engines-for-tejas-jets-on-purpose-8025363.html>
- 4 <https://www.eurasiantimes.com/india-ditches-us-gps-for-much-more-accurate-navic-navigation-system/>
- 5 Pandit, Rajat (17 November 2011). "Eyeing China, India to enter ICBM club in 3 months". The Times of India. India. Archived from the original on 19 April 2012. Retrieved 31 May 2012.
- 6 <https://www.space.com/india-anti-satellite-test-significance.html>
- 7 <https://journals.openedition.org/spp/1524>
- 8 Giuseppe, Gagliano (2018-01-31). "Historical aspects of the economic warfare in the interpretation of Christian Harbulot". Modern Diplomacy. Retrieved 2021-12-05.
- 9 <https://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>
- 10 "Echelon: Big brother without a cause". *BBC News*. 6 July 2000. Archived from the original on 7 January 2009. Retrieved 27 August 2006.
- 11 "Big Surveillance Project For the Amazon Jungle Teeters Over Scandals". *The Christian Science Monitor*. Archived from the original on 3 March 2016. Retrieved 15 October 2013.
- 12 David E. Sanger and Tim Weiner (15 October 1995). "Emerging Role For the C.I.A.: Economic Spy". *The New York Times*. Archived from the original on 10 July 2019. Retrieved 15 October 2013
- 13 Schmid, Gerhard (11 July 2001). "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))" (PDF). Archived (PDF) from the original on 28 June 2019. Retrieved 6 August 2018.
- 14 Staunton, Denis (16 April 1999). "Electronic spies torture German firms". *The Irish Times*. Archived from the original on 21 September 2018. Retrieved 6 August 2018.

- 15-17 https://en.wikipedia.org/wiki/Economic_Espionage_Act_of_1996
- 18-19 https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act
- 20-21 https://en.wikipedia.org/wiki/CLOUD_Act
- 22-24 https://en.wikipedia.org/wiki/Patriot_Act
- 25-28 https://en.wikipedia.org/wiki/UKUSA_Agreement
Greenwald, Glenn; MacAskill, Ewen (June 6, 2013). "NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files
29 Reveal – Top-Secret Prism Program Claims Direct Access to Servers of Firms Including Google, Apple and Facebook –
Companies Deny Any Knowledge of Program in Operation Since 2007 – Obama Orders US to Draw Up Overseas Target List
for Cyber-Attacks". *The Guardian*. Archived from the original on February 7, 2019. Retrieved June 15, 2013.
- 30 Seipel, Hubert (January 26, 2014). "Sweden Interview: Transcript". *Norddeutscher Rundfunk*. p. 3. Archived from the
original on January 28, 2014. Retrieved May 6, 2019.
- 31 <https://www.electrospace.net/2014/01/slides-about-nas-upstream-collection.html>
- 32 <https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>
- 33 https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html
- 34 <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>
New York Times, AT&T Helped U.S. Spy on Internet on a Vast Scale & Pro Publica, NSA Spying Relies on AT&T's 'Extreme
35 Willingness to Help', August 15, 2015.
- 36 Ball, James; Borger, Julian; Greenwald, Glenn (September 5, 2013). "US and UK spy agencies defeat privacy and security on
the internet". *The Guardian*.
- 37 Cox, James (December 2012). "Canada and the Five Eyes Intelligence Community" (PDF). RINJ Press. Retrieved 22
January 2020.
- 38 Intelligence in the Internet Era – Studies in Intelligence Archived 2007-04-22 at the
- 39 Julianne Pepitone (18 March 2014). "NSA Can Record All of A Foreign Country's Calls: Report". NBC News.
- 40 <https://www.wired.com/2015/08/know-nsa-atts-spying-pact/>
Schmid, Gerhard (11 July 2001). "On the existence of a global system for the interception of private and commercial
41 communications (ECHELON interception system), (2001/2098(INI))". European Parliament: Temporary Committee on the
ECHELON Interception System. Archived from the original on 26 December 2013. Retrieved 5 January 2013.
- 42 Budiansky, Stephen (2016). *Code Warriors*. New York: Alfred A. Knopf. pp. 23, 286–291. ISBN 9780385352666.
- 43 "10 U.S.C. § 467 : US Code - Section 467: Definitions".
- 44 <https://www.nsa.gov/Signals-Intelligence/Overview/>
- 45 https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/chatter_patterns.pdf
- 46 New NSA leaks show how US is bugging its European allies, *The Guardian*, 30 June 2013. Retrieved July 2013.
- 47 Bamford, James (2008). *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York
City: Doubleday. ISBN 978-0-385-52132-1. p. 325–340.
- 48 Spiegel Online (28 October 2013). "Photo Gallery: Spies in the Embassy". *Spiegel Online*. Archived from the original on 24
February 2014. Retrieved 22 March 2014.
- 49 https://commons.wikimedia.org/wiki/File:Boundless_Informant_data_collection_-_DNI.jpg
"US spy centre in India too". *Deccan Chronicle*. 30 October 2013. Archived from the original on 2 February 2014.
50 Retrieved 31 January 2014.
- 51 <https://www.space.com/41868-spacex-gwynne-shotwell-answers-weapons-question.html>
Freedberg, Sydney (20 August 2018). "Space-Based Missile Defense Can Be Done: DoD R&D. Chief Griffin". Archived from
the original on 29 September 2019. Retrieved 1 January 2020.
- 52 <https://spacenews.com/space-development-agencys-data-transport-satellites-get-more-complex/>
- 53 <https://spaceimpulse.com/2024/02/21/spacex-is-strengthening-national-security-ties-the-wall-street-journal-reports/>
- 54 <https://www.iqt.org/portfolio/>
- 55 <https://www.theverge.com/2023/9/28/23894239/spacex-starshield-satellite-network-space-force-pentagon-deal>
- 56 <https://www.theverge.com/2023/9/28/23894239/spacex-starshield-satellite-network-space-force-pentagon-deal>
- 57 <https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16>
- 58 Erwin, Sandra (5 October 2020). "L3Harris, SpaceX win Space Development Agency contracts to build missile-warning
satellites". *SpaceNews*. Archived from the original on 27 June 2021. Retrieved 1 December 2021.
- 59

- 60 <https://www.dvidshub.net/image/5272542/spacex-ceo-visits-local-commands>
- 61 <https://www.rfsafe.com/starlink-5g-cell-towers-in-space-get-full-fcc-approval-to-beam-71-76-ghz-to-earth-and-81-86-ghz-to-space/>
- 62 <https://twitter.com/elonmusk/status/1695475565510459643>
- 63 Yuan-Zhen et al, Beijing Institute of Tracking & Telecommunication Technology; Beijing Institute of Radiation & Measurement Technology, doi:10.3969/j.issn.1009-086x.2022.02. 002 Vol 50, No2, April 2022, Modern Defence Technology
- 64 <https://starlinkinsider.com/starlink-gateway-locations/>
- 65 <https://missiledefenseadvocacy.org/defense-systems/space-tracking-and-surveillance-system/>
- 66 *Machi, Vivienne (1 June 2021). "US Military Places a Bet on LEO for Space Security". Space Development Agency. Archived from the original on 5 December 2021. Retrieved 1 December 2021.* This article incorporates text from this source, which is in the public domain.
- 67 Yuan-Zhen et al, Beijing Institute of Tracking & Telecommunication Technology; Beijing Institute of Radiation & Measurement Technology, doi:10.3969/j.issn.1009-086x.2022.02. 002 Vol 50, No2, April 2022, Modern Defence Technology
- 68 https://web.archive.org/web/20090629222921/http://www.ndu.edu/nwc/nwcCLIPAr/US_AIR_FORCE/Equipment/Space-related/ASAT_Wpns/usaf-space-asat.htm
- 69 <https://www.nytimes.com/2024/09/01/world/americas/elon-musk-brazil-starlink-x.html>
- 70 Bajak, Frank (February 9, 2023). "Musk deputy's words on Starlink 'weaponization' vex Ukraine". *AP News*. Archived from the original on April 28, 2023. Retrieved September 16, 2023.
- 71 <https://www.dailysabah.com/world/mid-east/no-starlink-for-gaza-after-elon-musk-bows-to-israeli-pressure>
- 72 <https://www.mintpressnews.com/elon-musk-starlink-helping-us-iran-regime-change-operation/283293/>
- 73 <https://www.thesling.org/the-antitrust-case-against-spacex/>
- 74 <https://www.lefigaro.fr/societes/airbus-va-supprimer-jusqu-a-2500-postes-dans-sa-branche-defense-et-espace-en-difficulte-20241016>
- 75 <https://edition.cnn.com/2024/05/04/asia/taiwan-starlink-intl-hnk/index.html>
- 76 <https://spacenews.com/the-coming-chinese-megaconstellation-revolution/>
- 77 <https://tass.com/science/1217351>
- 78 <https://www.isro.gov.in/>
- 79 <https://www.ibef.org/industry/telecommunications>
- 80 <https://www.f6s.com/companies/space/india/co>
- 81 <https://link.epo.org/web/Space-borne%20sensing%20and%20green%20applications%20report.pdf>
- 82 <https://www.investindia.gov.in/sector/space>
- 83 <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvbsbdihbGfGhdFgFHytyhRtMjk4NzY=>
- 84 https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
- 85 https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf
- 86 <https://www.starlink.com/business/direct-to-cell>
- 87 <https://news.az/news/macron-and-scholz-pledge-to-boost-european-sovereignty-following-trumps-victory>