SOPHOPOLIS CONSULTING

FirstNet – a work in progress

A nationwide public safety broadband network for the US – what could other nations learn?

2018-11-22

An updated and slightly edited version of a background memo originally written in the early fall 2018. Also added to the original report is a speculative chapter discussing what a FirstNet solution could look like in a Swedish context. The report is based on openly available information/material, with a strong focus on broad policy issues of possible relevance to other nations interested in establishing a nationwide mobile public safety broadband network.

1. FirstNet – a developing project well worth following

In the United States, implementation of the country's first nationwide public safety broadband network – **FirstNet** – has just begun.[1] With debates on the same theme already under way or soon to be expected in various parts of Europe (and elsewhere) the following memo is intended to serve as an introduction and backgrounder to the FirstNet project. Focus will be on policy relevant, strategic decisions shaping the network, including decisions on matters of governance and control.

*

Hopefully most information below is of relevance to the reader, but maybe not all of it for everybody. Given discussions in Sweden about public safety communications this memo includes a few "comments" highlighting some interesting facts or developments. Those comments will be clearly identified and *in cursive writing.* Moreover, since the descriptive part of the report was finished, a speculative chapter discussing what a FirstNet solution could look like in a Swedish context has been added and serves as some kind of comment in and of itself.

1.1. Early days – but lessons to be learned from strategic decisions

The practical implementation process is still in an early phase, but there are already a number of facts and experiences to make note of as regards both the conceptual thinking behind the FirstNet project and the recently initiated roll-out phase. Some interesting examples of strategic and/or operational decisions include decisions by the US government to:

- Build a public safety broadband network based on commercial standards, expecting the benefits of lower costs, a speedy roll-out, consumer-driven economies of scale and rapid evolution of advanced communication capabilities.
- Trust a commercial actor (AT&T), governed and held accountable by contractual arrangements and institutional oversight, to build and operate a robust, secure, dedicated, separate public safety network largely based on existing commercial structures.
- Provide the commercial entity (A&T) with the right to use a part of the 700 MHz spectrum (Band 14) dedicated for public safety for the duration of the contract.
- Allow the commercial entity to use public safety spectrum capacity for its commercial operations as long as the capacity is not required for public safety operations.
- Arrange for governance and control by creating an independent government authority responsible for realizing the project under the directions of a board appointed by the Secretary of Commerce. In addition, parliamentary oversight is established via yearly audits and reports provided to relevant committees of Congress.

Together with the appointed commercial operator - AT&T – the government, primarily represented by the FirstNet Authority, have also made some interesting operational decisions to:

- Allow immediate usage of AT&T's commercial network for FirstNet subscribers in order to kick-start the operational phase as well as to provide for good redundancy.
- Quickly adapt the FirstNet market strategy in response to changing market conditions already in the early roll-out phase (more on this below).

[1] The term FirstNet has come to refer to both the actual network being built, the public-private partnership between the FirstNet Authority and AT&T, and the FirstNet Authority running and controlling the endeavour.

Fully operational on local levels

The roll-out is only in its initial phase, but given the ability for public safety users to use AT&T's commercial spectrums from day one, and the possibility to request deployable network assets, FirstNet has already been leveraged by a number of subscribers in various disaster and crisis operations. Among those are this summer's wild fires in western US, the hurricanes Florence and Michael in the East (e.g. Florida and Georgia) and a search and rescue operation in a remote tribal area in North Dakota.[2]

1.2. A word of caution

For the moment a lot of positive noise is made about the FirstNet project, not least by AT&T and the FirstNet crew itself. However, it is still very much a work in progress. The earliest anticipated date for the FirstNet nationwide network to go live is 2020, and the date when the project is to be steadily funded by subscription and leasing fees is well into 2022. The new capabilities being installed in the current roll-out phase are only being tested, and there are sceptics - including public safety communications experts - who doubt that the system will ever work as intended, primarily due to administrative and economic challenges specific for the US.

Moreover, it can be noted that by the end of this summer and during fall there has been major changes to both the operational leadership and to the board. Shortly after the resignation of the chairman of the FirstNet Board, and of her deputy, the CEO of FirstNet also left his post. Since then new people have been appointed and in line with the regulations about a third of the board members have also been rotated out and succeeded by new people. There is no information available to suggest that the resignations were prompted by any severe problems, but given the scale of the turnover something may be amiss - a development well worth following.

A changing public safety communications landscape necessitates adaption

As regards the market adaption decisions mentioned above, already deemed necessary by FirstNet, this is probably not relevant for most other countries since the US situation is quite unique. Historically a number of carriers have offered public safety mobile solutions to regional and local authorities, with the largest carrier – Verizon - being the market leader also for public safety networks. Given specific circumstances in the US, local and regional actors are free to choose any network they want, or to refrain from buying such services at all.

Unlike what would possibly be the case in most other nations, Verizon is now actively competing with the government sponsored alternative (FirstNet), offering very similar services. The changing crisis communications landscape is also affected - at least temporarily - by much discussed mishaps (on the part of Verizon) in connection with recent wild fires. In response to this development both AT&T and Verizon are currently trying to adapt their public safety offers and their marketing.

[2] https://www.rrmediagroup.com/News/NewsDetails/NewsID/17526; https://urgentcomm.com/2018/10/31/trick-or-treat-next-few-months-could-influence-direction-of-critical-communications-world/

2. FirstNet's history - a long road from idea to reality

2001 – 2017: A long, slow process

After the terrorist attacks of 9/11 in 2001 there was general agreement on the need for a national public safety broadband network (NPSBN) in the U.S. But setting something like that up in the geographically huge, administratively disparate and economically very competitive US market with highly autonomous state and local authorities proved to be very challenging. It wasn't until spring 2012 that a formal decision was made and Congress enacted **The Middle Class Tax Relief and Job Creation Act of 2012** - a law containing landmark provisions to create a first responder network.[3]

According to the law, the network should be based on modern wireless technology (LTE) and make use of a dedicated broadband spectrum (700 MHz, Band 14). To finance the first deployment phase of the build-out the law provided $7 billion in funding. For the purpose of governance of both the build-up phase and the long-term operations of the new network the law stipulated the creation of a framework in the form of the new "First Responder Network Authority", defined as an independent authority hosted within the Department of Commerce.

In spring 2017, after five more years of planning, requests for proposals and deliberations, the FirstNet Authority could finally award the contract to build and operate the first responders' network (FirstNet)[4] - to the nation's second largest wireless carrier, AT&T[5]. As part of the deal, a public-private partnership was formed and now runs the project, based on agreed upon conceptual thinking.

2018: With the whole country on-board, the initial roll-out phase begins

In accordance with the 2012 law, each of the 56 states and territories were offered to opt into the FirstNet project, but they did not have to, and for a while it looked as if some were to opt-out. But by the deadline, at the end of 2017, all 50 states and three territories had opted in, with the remaining three doing so in January 2018.

By spring 2018 FirstNet announced that AT&T had delivered, on schedule, upon the promise to complete "a dedicated public safety LTE evolved packet core", also described as the brain of the network. FirstNet/AT&T will, however, continue testing the core before it is used by public safety subscribers on a widespread basis. Early in the year AT&T also started the roll-out of the network by equipping and upgrading infrastructure (primarily old and new cell-sites) to enable the use of the dedicated 700 MHz spectrum (Band 14). The roll-out is still in an early stage but is publicly said to exceed the base scenario as regards both the number of subscribers signing up and the amount of PS-LTE equipment being put up to improve the reach and expand the performance of the network.

But, as mentioned in the introduction, FirstNet is still far from fully operational. Meanwhile, first responder entities and individuals who sign up as subscribes are offered full use of AT&T's existing commercial network, including extra services such as prioritization of public safety traffic and pre-emption of other traffic.

---

[3] The seemingly odd legal context (tax relief and job creation) is due to an American practice of political manoeuvring, where a legal provision is included into a not very relevant law, either for practical reasons or because a group of congressmen make such a move a condition for their support.

[4] Comprehensive and current information on the FirstNet project can be found on the FirstNet Homepage.

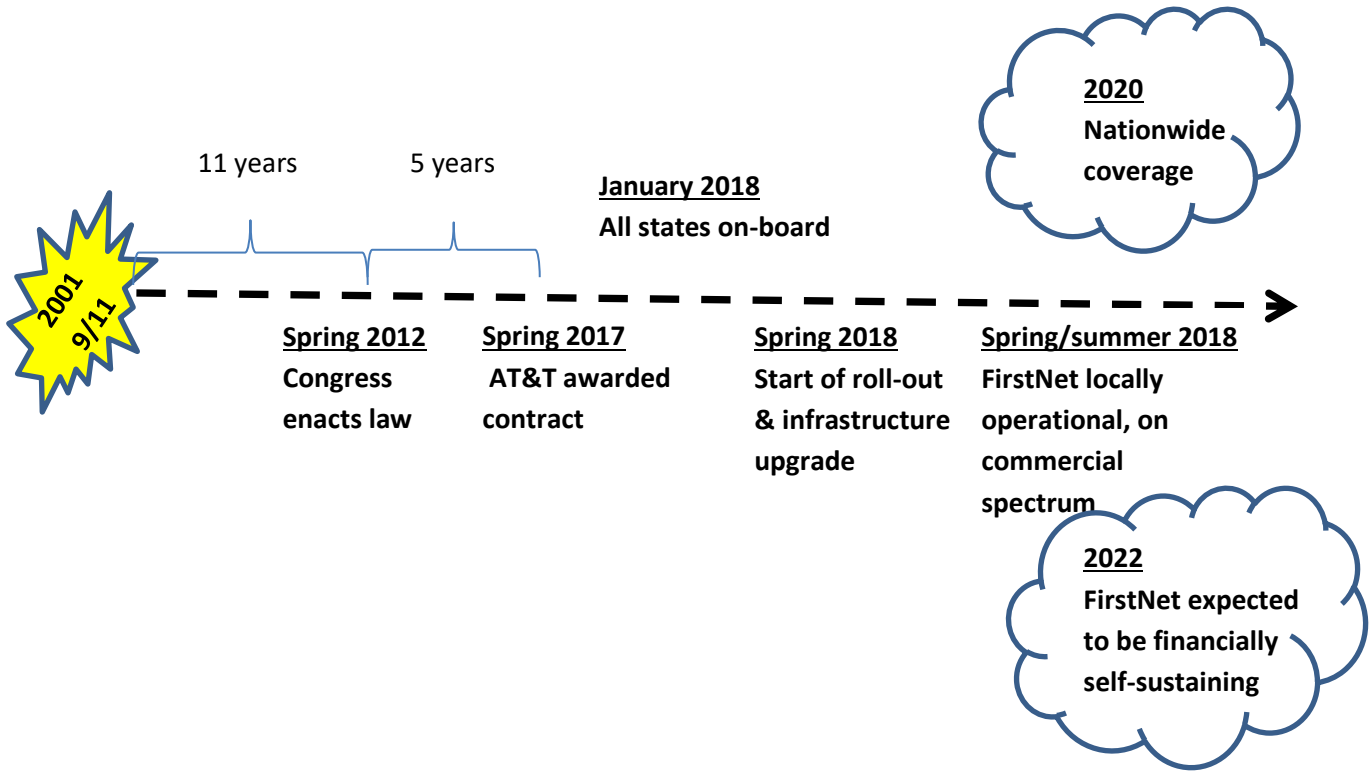
[5] Verizon, the market leader in both commercial mobile and public safety communications, decided not to bid for the contract, partly since it saw no need for extra spectrum.

Comment: This practice illustrates the fact that carriers are perfectly able, technically, to offer priority and pre-emption even on the commercial networks. Verizon is doing the same thing, vividly defending its market position, but was recently hit by severe negative criticism after first responders fighting wild fires had their communications limited in line with their subscriptions that contained caps on data transfer (just like many private subscriptions do). Verizon has since seen itself forced to make apologies and to promise first responders, media and politicians that they will now offer limitless data transfer to all their first responder subscriptions – without any extra charges. As could be expected AT&T is making a big thing of Verizon´s mistake and now continuously points out that FirstNet subscribers - unlike Verizon's customers - will never run the risk of having their communications "throttled" (the prevailing term for intentional reductions of customers' transmission capacity).

*

21 years in one picture

As the picture below is intended to illustrate, the decision making process leading up to FirstNet was very long and slow (11+5 years). But once the formal contract was signed AT&T and the FirstNet authority have been able to act rather quickly. If all goes according to plan public safety authorities all over the US will be able to subscribe to a dedicated nationwide mobile broadband network only three years after the contract was in place. And in the meantime those who want to can use a growing amount of services and applications over commercial networks.



3. The FirstNet Concept

Using the wording of Congress' legal act itself:
"*The First Responder Network Authority shall ensure the establishment of a nationwide, interoperable public safety broadband network … based on a single, national network architecture that evolves with technological advancements*".

The legal act also states that the network initially shall consist of, among other things:

- *A core network consisting of national and regional data centers, and other elements and functions that may be distributed geographically, all of which shall be based on commercial standards; and that provides the connectivity between the radio access network and the public Internet or the public switched network, or both*.
- *A radio access network that consists of all cell site equipment, antennas, and backhaul equipment, based on commercial standards, that are required to enable wireless communications with devices using the public safety broadband spectrum...*

The law also states that the FirstNet Authority, when requesting proposals for the main contract to build, maintain and operate the network, shall encourage that "*such requests leverage, to the maximum extent economically desirable, existing commercial wireless infrastructure to speed deployment of the network*".

3.1 The Contract

The agreement between FirstNet Authority and AT&T has not been made public but is known to cover a period of 25 years and to state that AT&T shall build and manage the FirstNet network while the FirstNet Authority will provide the 20 MHz spectrum (Band 14) plus success-based payments of $7 billion over the next five years to support the build-out. AT&T is to spend about $40 billion over the life-time of the contract to build, deploy, operate and maintain the network.

Addressing the rural divide

In its decision of 2012 Congress also stated clearly that the FirstNet Authority, when choosing the commercial actor to build and operate the network, should require deployment phases with substantial rural coverage milestones as part of each phase of construction and deployment.

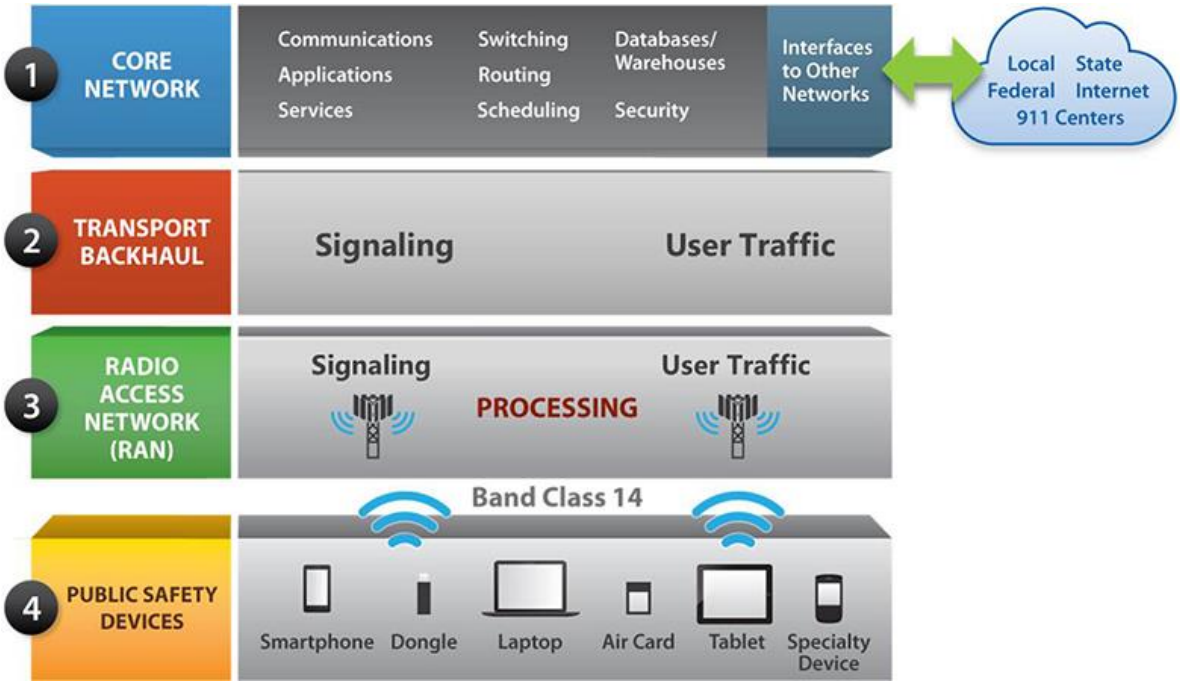
National security restrictions

In the 2012 law establishing FirstNet it is clearly stated that national security restrictions apply to the realization of the FirstNet project, both as regards commercial entities/persons bidding for contracts and/or receiving funding.

3.2. The FirstNet-concept of today

The Network Architecture

Naturally, the conceptual thinking has evolved since 2012. Today, FirstNet broadly defines the network in four distinct layers: the core network; the transportation backhaul; the radio access network and the public safety devices (like smartphones, tablets, lap-tops and specially developed public safety devices).



FirstNet's basic building blocks [6]

Layer 2, 3 and 4 are rather self-explicatory, but the so called core network concept holds some interesting challenges and solutions that will be discussed below.

The core network: The brain and the separating mechanism

The information provided by the FirstNet Authority and AT&T is somewhat nebulous when it comes to the core network (the first layer). It is often described as the brain of the network and contains functionalities like data storage, switching, routing, processing and reformatting. In addition to constituting the interface to other networks, like 911 and the Internet, the core is also the part of the network where cyber security is to be established.

The core is solely dedicated to the public safety mission and is built on hardware physically separated from AT&T's commercial systems. It is on this solution that FirstNet and AT&T base statements about FirstNet being a dedicated, separated public safety network even though a lot of the infrastructure is the same as in AT&T's commercial operations.[7]

The Transportation backhaul

In general terms the Transportation backhaul (the second layer) is the nation-wide fiberoptic back-bone of the network – often described as "*the links that carry user traffic, such as voice, data and video, and signalling from the radio base stations to the core network*."

[6] http://firstnetme.gov/process/deployment.html

[7] According to the 2012 law, the core network can consist of national and regional data centres, and other elements and functions that may be distributed geographically. To what extent the core really is or will be multi-centred and geographically distributed is currently unclear.

The Radio Access Network and Devices

AT&T is in full swing deploying new cell sites as well as upgrading old ones to enable the use of the 700 MHz Band 14 spectrum. According to the company's own estimates the buildout will be much faster than the contracted five years for most of the U.S.

FirstNet-enabled devices do already exist and are expected to multiply the coming years, their functionality amplified by a large number of new applications. Existing and future applications will have to be certified by the FirstNet Authority and will then be available for subscribers to download from FirstNet's own "app store".

*

Separate or not separate – that is the question…

Apart from the core and its physically separated hardware, FirstNet's traffic will flow via much of the same infrastructure as AT&T's commercial traffic. An obvious exception is in remote areas where new infrastructure and capacity will be built in order to fulfil the contractual levels of FirstNet coverage (coverage ambitions often cited are 99 % of the population and 95 % of the territory, or 99% of the highway system).

Comment: The contractual demands on AT&T to expand coverage has been an important policy object for the government since it has positive effects on the overall digitalization of the country and on the ambition to develop rural areas. AT&T openly states that they use the deployment and upgrading of Band 14 infrastructure (4G LTE standard) to simultaneously prepare cell-sites and other infrastructure for commercial 5G-traffic, thus saving themselves time and money in the budding 5G-race.

4. Governance & control

As already mentioned the law establishing what has then become FirstNet stipulates the creation of an independent authority (the FirstNet Authority) to be housed within the Government (Department of Commerce) but led by an independent board with 15 members appointed by the Secretary of Commerce. This structure constitutes the main governance and control apparatus and will be briefly described below.

A contractual governance approach

Another important aspect of the governance challenge refers to ownership and control over infrastructure as well as software, information and daily operations of a network. In the case of the US and FirstNet, the solution was to trust a commercial company, AT&T, to move forward in tandem with the FirstNet Authority based on a contractual arrangement detailing AT&T's responsibilities to build, develop, maintain and operate FirstNet.

4.1. Department of Commerce: NTIA & OPSC

The Secretary of Commerce (Wilbur Ross) is the government member formally responsible for FirstNet. Within the Commerce department FirstNet-matters are primarily the responsibility of the Assistant Secretary for Communications and Information, David Redl, who also serves as the administrator for the National Telecommunications and Information Administration, NTIA, which houses the independent authority FirstNet within the U.S. Government.

NTIA is the executive branch agency principally responsible for advising the President on telecommunications and information policy issues. NTIA focus largely on expanding broadband internet access and adoption in the US. The implementation of NTIA's responsibilities under the 2012-law (the Middle Class Tax Relief and Jobs Creation Act) is overseen by the Office of Public Safety Communications (OPSC). OPSC also supports the FirstNet Authority with its procurement efforts and other administrative support functions.

4.2. The FirstNet Authority

Even if supported by the Department of Commerce's NTIA/OSPC, the FirstNet Authority is an independent entity with its own executive leadership normally consisting of seven chief officers (the CEO resigned early September 2018 but has since been replaced)[8].

The FirstNet Authority is tasked with ensuring the establishment of a nationwide interoperable public safety broadband network and is, in this capacity, the single nationwide licensee of the 700 MHz public safety broadband spectrum (Block 14), the usage of which is transferred to AT&T for the duration of the co-operation. AT&T's right to use the Block 14 spectrum will to be reviewed after 10 years.[9]

[8] Short bios and pictures of the chief officers can be found on FirstNet's website: Leadership.

[9] According to the 2012 law the FirstNet Authority will initially hold the license for 10 years after which it shall apply to the Federal Communications Commission (FCC) for a renewal of the license. Given that FirstNet has met its duties and obligations, the FCC can grant a renewal of the licence for a term of no more than 10 years.

However, The FirstNet Authority is more than just the government side of the partnership, and should also bring significant public safety expertise, experience and relationships to the table. Moreover it is meant to be the voice of the public safety sector regarding development and deployment of the network, not least as regards the possibility for regional and local actors to bring input forward.

The FirstNet Authority has a 15 years mandate, running from 2012 to 2027. No later than 2022 the Comptroller General of the United States shall submit to Congress a report on what actions to take regarding this sunset clause.[10]

Committees of the FirstNet Authority

To be assisted in carrying out its duties and responsibilities the FirstNet Authority shall establish a "standing public safety advisory committee", and may also establish additional standing or ad hoc committees or panels as it determines necessary.

4.3. The FirstNet Board[11]

The 2012 law states that FirstNet Authority shall be led by a Board consisting of the Secretary of Homeland Security, the Attorney General, and the Director of the Office of Management and Budget as permanent members plus 12 more individuals appointed by the Secretary of Commerce. In making these appointments the Secretary shall:

- appoint no fewer than 3 individuals to represent the collective interests of the States, localities, tribes and territories;
- seek to ensure geographic and regional representation in such appointments
- seek to ensure rural and urban representation in such appointments
- appoint no fewer than 3 individuals who have served as public safety professionals

Each appointed member must be an American citizen and meet at least one of four qualification criteria: public safety experience; technical expertise; network expertise; financial expertise.

The Board shall meet at least once every quarter of the year and at the call of the chair. The Board meetings, including any sub-committee of the Board, shall be open to the public. By majority vote the Board may, however, close a meeting for the time necessary to preserve the confidentiality of commercial or financial information or to discuss personnel or legal matters.

Comment: In order to have some continuity the initial appointments were staggered, with different terms to serve for some of the members. As a result, and amplified by two recent resignations (chair and vice-chair there were up to six (out of fifteen) seats to fill, this fall – providing the Secretary of Commerce and the Administrator of NTIA with an opportunity to shape the composition of the board to their liking. New board members were appointed late October, but until now there have been no signs of overly politicized appointments.

[10] The FirstNet Authority has its HQ in Virginia but in the implementation phase many practical FirstNet-related matters are handled by either AT&T's headquarter in Texas or, in more technical matters, by FirstNet's/AT&T's technology headquarter and test lab in Boulder Colorado (employing 50 people).

[11] More information regarding members, meetings, resolutions and sub-committees can be found on the Board's homepage: https://www.firstnet.gov/board.

4.4. Parliamentarian oversight

There are also some paragraphs in the 2012 law providing for parliamentary oversight via audits and testimonies.

Yearly audits

Apart from the FirstNets Authority's standing mission to oversee the development, deployment and running of the FirstNet network, the Secretary of Commerce shall arrange for yearly audits by an independent auditor. The audits shall be made available to relevant committees of Congress.

Yearly reports to congress

Also, the FirstNet Authority shall submit an annual report covering the preceding fiscal year to the appropriate committees of Congress. The report shall include a comprehensive and detailed report of the operations, activities, financial condition and accomplishments and recommendations for legislative or administrative action.

5. A brief note on the theme of a changing market

5.1. A growing market

Public safety LTE (PS-LTE) networks are underway or in operation in a number of countries all over the world (US, UK, South Korea, Australia, Qatar and others). Analysts assess that several billion dollars will be spent annually on PS-LTE infrastructure, and referring to leading analyst companies such as Gartner, HIS and SNS, recent suggestions have been made that until 2021 the number of subscribers will jump from about 2 million to over 10 million, and PS-LTE service revenue grow to over 10 billion per year. Another stream of revenue (2 billion dollars by 2021) is anticipated to be generated via a multitude of new services and applications currently being developed to run on public safety devices.[12]

Precisely along this line of reasoning, AT&T representatives have been open about the fact that its FirstNet role could lead to additional sales opportunities beyond providing a single broadband link to individual first responders. For example they see one first responder as a potential user of three or four connected points (devices), like a phone, a body camera, a vehicle mounted device or a drone. There are also plans to attract subscribers among in-house personnel, like dispatchers, people at strategic facilities (hydro dams, airports, ports) or support service providers (energy and water providers).

5.2. The practical roll-out – an update

At a press conference in late July AT&T declared it had installed equipment operating in the FirstNet spectrum band on 2 500 cell sites – a claim that still awaits validation from the FirstNet Authority.[13] It was also stated that the FirstNet spectrum band (Band 14) was operational for testing purposes in more than 40 states; that Band 14-capable devices were eligible to first responders; and that FirstNet dedicated deployable networks (for example truck mounted cell-sites) were available in case of a need to boost coverage during large events and emergencies.

According to AT&T around 1 500 public safety agencies (out of maybe more than 200 000 nation-wide) had signed up for FirstNet by the end of July, accounting for more than 110 000 connections/subscriptions. By the end of October media reported that the number of agencies and subscribers had continued to grow more than expected and had now reached 3600 public safety agencies, making the total number of subscriptions more than 250 000.

The enrolment tempo is said to have increased dramatically during August and early September, partly due to the renewed attention given wild-fires but also due to AT&T adapting their offer to clients to make a subscription more attractive. For example more volunteer first responders (very common in the US) are now eligible for a FirstNet subscription. And given practical realities for many small first responder entities (no money, lots of volunteer work) it is now possible to use private devices (BYOD). In parallel AT&T are offering individual first responders competitive private deals on new smartphones and other devices ready to be used on the Block 14 spectrum.

[12] One proposed new service is Mission Critical Push to Talk (MCPTT), designed to provide LMR-like services which may eventually let first responders carry only one device to access voice, data and video.
[13] Over time AT&T expects to deploy FirstNet enabling equipment on more than 10 000 more cell sites, most of them on existing sites.

6. Food for thought: FirstNet governance in a Swedish context

Needless to say, there are many differences between Swedish and American prerequisites as regards public safety and telecom. Nevertheless, since both nations are aiming for a secure, future-proofed public safety network characterized by adequate governmental control and governance, valuable insights might emerge from an experimental direct translation of the FirstNet governance concept into a similar Swedish blue light network context ("BlueNet" in the following).

One particularly interesting question is to what extent a nation chooses to leverage the skills and existing infrastructure of commercial actors for building and operating a modern public safety network. A growing number of nations have already started planning and/or establishing 4G/LTE public safety networks and so far all of them seem to have chosen to involve commercial operators to a large or at least rather large extent (USA, UK, Finland and France). Naturally, no governance solution looks the same in those different countries, but one way or the other they all appear to rely on contractual control and governance of commercial operations. As for the security aspect, redundancy through commercial networks is a centre piece of most, or maybe even all, different concepts.

6.1. Governance

On a brief and speculative note - assuming necessary administrative and legal constructions are put in place- a Swedish "BlueNet" could possibly be organized in the following way:

6.1.1. The Government & government agencies

Just like with FirstNet in the US, the Swedish Government could decide to create a more or less independent authority (the "BlueNet Authority") tasked to establish and oversee the operations of a Swedish "BlueNet". Such an entity could preferably be hosted within (or even be an integral part of) the relevant government agency (MSB), which in turn is tasked and funded by one of the ministries (currently Justice, potentially Defence).

The security aspects will be elaborated on below, but in the governance context it should be noted that the authorities should have no problem to include demands on commercial actors as regards restricted access to sensitive data or localities and on the use of vetted personnel with adequate security clearance. Contracts could also include the right for authorities to audit security processes both before a contract is signed and later, when services are being delivered. Similarly, learning from what is currently happening in the US, Swedish authorities could also include demands on carriers bidding for the "BlueNet" project that they provide the public safety agencies with mission critical capacity (prioritization, prevention etc.) also over their commercial 4G/LTE and 5G/NR frequencies.

6.1.2. The "BlueNet Authority"

The "BlueNet Authority" would have to plan for, negotiate and procure both the build-up and the running of the operations of the network from commercial actors. MSB and the "BlueNet Authority" would also be the government's instrumental vehicle for controlling that contractual agreements are fulfilled and that the commercial actors are held accountable. In addition, the "BlueNet Authority" would also be in control of the development of a platform for various applications (an app-store), where BlueNet users could download evaluated and certified BlueNet-apps (for example special map services, push-to-talk-apps for smartphones etc).

The contract

The contractual agreements could be rather strict and could include, for example, clear delivery targets regarding coverage (e.g. geography, population), technology capabilities, build-out of rural areas etc.[14] Moreover, there would have to be rules and procedures to guarantee the "BlueNet Authority" and the Government a satisfactory control over what commercial partners take part in building or operating the network, including cases where ownership or control over a private entity changes (for example a little known sub-contractor).

A well thought through plan for the ownership of various dedicated assets would also strengthen the Government's control if/when the issue of changing commercial partners comes up or if other challenges arises regarding the change of control at any level of the commercial eco-system underpinning the "BlueNet" operations. In the case of FirstNet, US authorities have also stipulated that the operator (AT&T) must assure that there is a certain number of suppliers of devices (phones, tablets etc.) so as to assure a healthy level of competition.

Spectrum ownership gives the government bargaining and governance power

One important aspect in this context is the American solution to keep the ownership of the dedicated spectrum with the FirstNet Authority, allowing the commercial operator to use the spectrum only as long as the contract runs (but for both public safety and – when not needed by public safety – commercial traffic). This set-up means that there would be a very high price to pay for an operator that fails to follow through on its promises or does not allow for a good degree of governance, potentially losing the contract. At the same time the solution offers effective usage of scarce spectrum and provides for a great deal of redundancy and, thus, resilience/security.

Apart from the spectrum, ownership of assets like reserve power units and cell-sites built for the Government (to establish commercially non-viable coverage for BlueNet) could also be placed with the "BlueNet Authority".

6.1.3. The "BlueNet Board"

The MSB would be ideally positioned to host a "BlueNet Authority" due to its current coordinating role, and would be ideal when it comes to identifying appropriate candidates for a board representing a good mix of public safety practitioners, experts and representatives from central/federal functions as well as relevant businesses. Following the American example one could expect to find 2-3 relevant Government ministers, representatives from the public safety agencies, from regional and local government (e.g. SKL), from the government offices as well as relevant industry representatives (industry associations)among the board members.

6.1.4. Parliamentary oversight

As for parliamentary control of a "BlueNet" there could, just like in the case of FirstNet, be annual audits and progress reports delivered to the relevant committees or groups within the parliament.

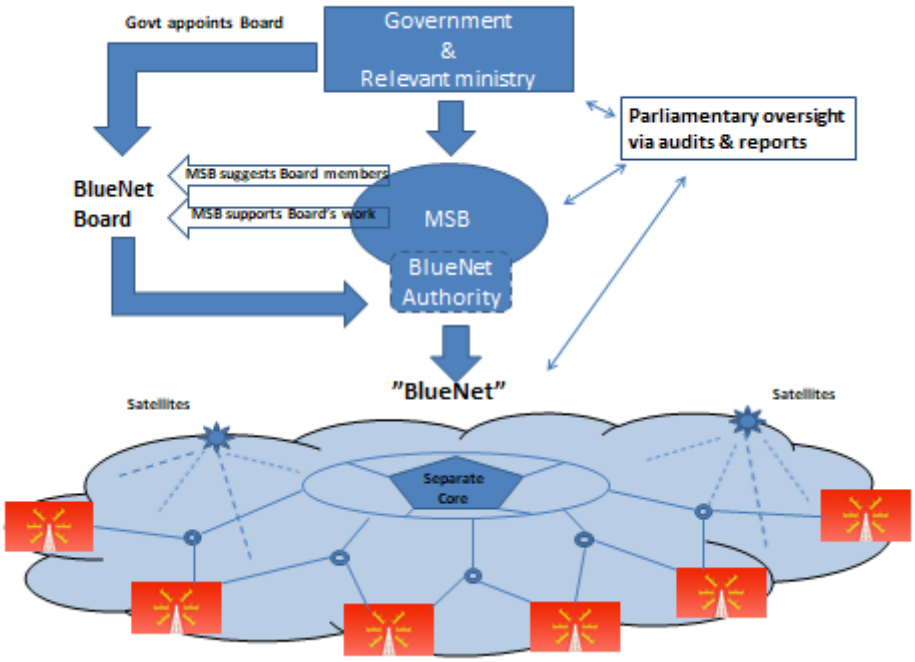
6.1.5. The BlueNet users

As competitive market actors, the telecom operators are forced to be highly customer oriented over time – thus willing and able to adapt and develop solutions for the constantly evolving digital society (in only a few years public safety 5G might be on the agenda, and then only large, competitive actors ready to invest and take business risks will be willing and able to deliver).In a "BlueNet" context the

[14] In the case of FirstNet, rural considerations are important since the roll-out of the commercially based network contributes to the digitalization of remote areas.

customers /users would not only be represented collectively via the Board and regular interaction with MSB. The users would also be able to engage on a more or less individual level (an organisation or local service for example) with the service provider who would be keen on holding on to the "BlueNet" contract over time. Thus, customer orientation would likely be an obvious aspect of a commercially based "BlueNet".

A rough schematic governance diagram



6.2. Security

Far-reaching security protocols and required administrative safety measures is nothing new for Swedish telecom companies with a long history of involvement in the so called "Total Defence" concept that is currently being revived. For decades, the Swedish Government and government agencies, including the Swedish police and defence, have been using commercial networks and services for sensitive communication – a practise based on contractual relations underpinned by trust, often built on long-term relations and a willingness within private companies to organize sensitive operations in a secure way with which the authorities are satisfied.

The antagonistic threat

What is new (or "renewed") is the potential threat from an antagonistic actor intent on disrupting critical infrastructure, including public safety services which are essential for a nation's resilience and security. Sweden, and many other modern nations, has seen a development towards economic efficiency and growth based on lean logistic chains and a high degree of dependency on networked information and communications technologies. As a result, protection against the effects of antagonistic attacks (cyber or kinetic) on the nation's fundamental functionality have been identified as an ever more important aspect of national security (both physical and psychological). And the solution to this threat is sought not by backtracking to an old-style inefficient society/economy but by increasing societal security and robustness.

In a modern, networked world: dependency = vulnerability; redundancy = security

However, in modern high-tech societies dependent on efficient networks (not only telecom, but also logistics, finance etc.) security and robustness is guaranteed just as much - or even more - by redundancy than by hardening potential targets in a network. Redundancy is crucial for modern day network security, and a well governed, commercially provided "BlueNet" reinforced by the ability to use other operators' networks (based on the very real interoperability we all make use of in our everyday communications) – would most likely be a much more secure solution than any stand-alone network based on a separate physical infrastructure.[15]

Also – just like in the US example – the virtual world provides options for a separate network based on a physically separate core (the system's brain, based on computers/servers separated from the commercial core). In addition, an evolving ability to "slice" network capacity into parallel "networks within a network" will bring about remarkable new possibilities down the road, especially when 5G is rolled-out. Again, this kind of opportunities will be available for customers of commercial operators long before they reach government owned and run, non-commercial networks.

Mitigating the risks of foreign access to sensitive information

Any risk of unwanted foreign involvement in the businesses taking part in the build-up and/or operational activities of a "BlueNet" could easily be mitigated by the kind of legal restrictions on foreign investments already in place or being discussed in most western nations as regards sensitive economic activities as well as national security concerns.[16] In the case of FirstNet, US authorities have put specific legal restrictions in place to prevent unwanted entities from bidding for FirstNet contracts or in other ways use investments to gain classified or sensitive insider information.

6.3. Conclusion: A "Swedish FirstNet" could provide advantages

Over time, close public-private cooperation managed by a contractual governance model has a number of advantages from society's point of view. First, and most obvious, is the high degree of cost-effectiveness when the authorities can make use of large, well tested and future-proofed commercial networks to achieve a quick and low-cost creation of a nationwide network. Similar benefits will apply during the operational phase, where costs for technological development and maintenance will be split with the operators' other, much larger, business activities.

Secondly (but just as important): Given the high degree of redundancy in the commercial networks, a FirstNet/BlueNet model could provide Swedish authorities with a high degree of over-all security which couldn't possibly be matched by no- or low-redundancy alternatives.

[15] In some nations the commercial operator with a public safety network contract also has agreements in place with other operators to use their networks in case of need.

[16] For example new SUA-rules in Sweden and expanded clout for the Cfius-regime (Committee on Foreign Investment) in the USA.