Submission:

Senate Foreign Affairs, Defence and Trade References Committee Human rights implications of recent violence in Iran

Introduction

What does this submission try to address

This submission is the author's testimony on the matters discussed in IRI embassy submission #19 (Additional information2).

The author's qualifications

The author has spent nearly 13 years in the telecommunication industry in Iran. During the last 5 years of his career in Iran (2014-2019), the author has served as the General Manager of Network Planning and Optimisation. The role was a direct report of the Network Executive and oversaw the Core Network, IP Network, and Terrestrial Transmission Network of Iran's second mobile operator which was also the largest provider of the internet in Iran.

Author's view on IRI

The author has tried to clarify which parts of this submission are the facts that the author has personally dealt with, and which parts are the author's opinions or speculations. Yet, for further clarity, the committee can refer to the author's previous submission #213 which explains the author's view on IRI.

The author believes that IRI is routinely using hostage-taking as a tactic to achieve its goals. Hostage Diplomacy is only one example. By presenting itself as a legitimate and normal nation-state, the aspiring sectarian empire takes more than foreign nationals as hostages. This submission is in part an attempt to reveal how IRI takes Iranians' access to the internet hostage.

What are IRI claims in submission #19 (Additional information2)

- IRI is the legitimate state of the Iranian nation and hence is entitled to law enforcement.
  [ISIS would have made similar comments had it been recognised as the legitimate state of Iraq and Syria]
- IRI law is compliant with international law. (Uses paragraph 3 of article 19 of ICCPR to justify restricting Iranians' access to the internet as lawful and necessary to protect national security, public order, morals and health.
  [The dispute is exactly about the term nation and what is meant by national security]
- IRI has not blocked Iranians' access to the internet and only blocked WhatsApp and Instagram
  [The committee can check with its reliable sources in Iran to see if this claim is true. Specifically, it would be nice if the sources can confirm whether platforms such as YouTube, Twitter, Meta, Telegram, … are accessible. Also, whether internet backouts, other than network outages, have happened over the past several years or not]
- Refers to the videos that have made it out of the restrictions as evidence that VPNs are working fine
  [The committee's reliable source in Iran can advise if most VPN services are functional or not]

- The restrictions are temporary and only to protect people's rights, with a focus on children's rights and to ensure children are not exposed to such violent content. IRI cares for the privacy of individuals, public order, and morals.
  [The committee can check with its reliable source in Iran, to see how many of the Iranians that have been murdered by IRI forces in the recent uprising were children.]
- IRI has provided Iranians with internet and expanded the access network to ensure Iranians will have good internet access.
  [The author shall attempt to clarify this in the rest of this submission]

To further access these claims that IRI has made, the author shall provide more information.

Some facts about ICT in IRI

Who does what in IRI when it comes to ICT

- Supreme Council of the Virtual Space (SCVS) was established on 7/3/2012. Khamenei commanded that this council must be formed. He appointed its members and dictated that whatever is passed by this council should be deemed as law (so much for the separation of power in IRI and the role of its parliament as the legislative branch). According to Khamenei's order, it was in part, formed to ensure IRI will be protected from that malaise of the internet. This council is where the implementation of the so-called National Information Network (NIN) became law. More on NIN will be discussed in this submission.
- ICT ministry Ministers are members of the cabinet and report to the president. Supposedly the highest role in the executive branch. [Of course, the incumbent Waly al-Faghih (a.k.a caliph), Khamenei can and does overrule the executive branch of IRI at will.]
- Communication Regulatory Commission (CRC) is the body that passes regulations for telecommunications. The parliament has delegated its authority to CRC to legitimise the regulations that it passes. Notably, the list of voting members includes representatives of the office of the chief of military staff (often from IRGC) and IRIB.
- Communication Regulatory Authority (CRA) is the regulatory authority that grants licenses to network operators and allocates frequency spectrum. It must ensure that all licensed operators are compliant with CRC regulations. In IRI, CRA is a part of the ICT ministry, and its head is one of the ICT minister's deputies.
- The Ministry of Intelligence is tasked by the SCVS with items 16, 28, 35, 38, 41, and 44 of a responsibility matrix that covers the list of high-level actions of the NIN master plan. (e.g., item 38 puts the ministry of intelligence in charge of "executing the appendix of control under the framework of the appendix of security of the NIN. More on this will be covered later in this submission)
- Telecommunication Infrastructure Company (TIC) is the provider of the infrastructure (mainly transmission links). Its charter is passed by the parliament and hence it is not a licensed operator. According to its charter, it has legal exclusivity on providing other players (mainly network providers a.k.a. operators who have been licensed by CRA) with connectivity to the

outside world (internet, international voice links, international singling links) and inter-province links and intra-province links of certain cities. This exclusivity is in practice the "infrastructure" of taking these resources hostage. More on this will be covered in this submission.

- Network operators are the providers of access networks. There are 3 mobile network operators and nearly 17 Fixed Communication Providers. They have obtained their licenses from CRA and must comply with its terms, conditions and appendices including two important ones: the Security Appendix and the Cultural Appendix. More on this will be covered in this submission.

A brief history of how IRI provided Iranians with new telecommunication technologies (Or lack thereof)

1979- 2014

Unlike what IRI claims in submission #19 (Additional Information2), for many years, telecommunication networks that were state-owned stagnated. The 2G mobile was launched only in 1993, 20 years after the first mobile call was made.

Iranians had to wait for 8 years after the invention of the Short Message Service (SMS) until finally, the IRI state-owned company offered it in 2002. Later in the protests that happened after the presidential election and while thanks to IRI, the only available mobile internet in the country was still 2G and most protesters relied on SMS to coordinate rallies, IRI authorities shut down SMS for more than 40 days in Tehran.

It took IRI, 8 years after the first 3G network was commercially launched in 2001, to grant its first 3G license to the third mobile network operator in the country. This operator enjoyed the usual two-year exclusivity period but failed to commercially launch its network until the next two years and IRI extended their exclusivity for nearly 4 more years and only allowed the serious players to offer 3G and 4G services in late August 2014 (after the concept of NIN was born). Until 2014, any mobile subscriber who wished to have access to more than 128 Kbps, had to register separate forms and bring in evidence such as a letter from their workplace explaining why they want to have access to the internet with a speed higher than 128 Kbps. The operator that had exclusivity on 3G technology from 2009 until 2014 was banned from offering video calling on 3G because of a fatwa that asserted such calls are religiously forbidden (haram).

The author has been involved with the ICT industry in Iran since late 2006. During this period, people in the ICT industry used to jokingly call the ministers such as Soleimani, Taghipour, and Nami, the minister of "disconnectivity".

Post-2014

The author speculates that after the SCVS and the concept of NIN were born, IRI had a change in its telecommunication strategy. Perhaps inspired by some of their friends in CCP, IRI seemed interested in allowing the access network providers to finally adopt new technologies and expand their networks such that IRI can utilise digital means for governance. Albeit, under its tight digital grip.

In an unprecedented move, the ICT minister of the time started weekly meetings with all fixed and mobile operators on NIN. The author represented his company in several such meetings and testifies that all the network expansions that happened in this period were carried out under the name of expanding NIN. Unlike what IRI has claimed in submission #19 (Additional Information2), IRI was not into expanding internet access for Iranians. Officially, it was chasing the idea of building NIN. A network that first and foremost provides IRI with digital services, "independent" of any other

country. It is noteworthy that internet access is only 1 out of the 30 services that are listed as what NIN should provide according to the SCVS NIN master plan (service item 19).

During this period, network providers tried to take advantage of the opportunity and expand internet access networks but officially, everyone reported the progress of their "NIN" projects.

Meanwhile, in line with its NIN-related responsibilities, the ICT ministry showed a lot of focus on launching local Internet eXchange (IXP) switches and forcing all network operators and web hosting/CDN service providers to build bilateral peering on these switches that were hosted by TIC. The idea was presented as a means to shorten the path between users and web hosting/CDN service points, increase reliability by removing the international links, and reduce the cost of operators who had to lease international bandwidth from TIC (the exclusive provider of international links). Prima facie, it could have been a good initiative, but this enabled IRI to cut international links and hence internet access while keeping access to local websites up and running. This proved to be one of the key initiatives of the NIN. A concept that the ministry insisted was not there to eventually replace the internet with an intranet.

Another initiative that the ICT ministry took, despite serious resistance from operators was passing a regulation in CRC to enforce operators to charge the bytes that a subscriber sends or receives based on the content. The regulation demanded operators charge the subscribers 50% of the usual price if they are using local content and 33% if they are using a local Over The Top (OTT) messenger application. A regulation that was a clear violation of Network Neutrality. Supposedly, to take a protectionist approach to support local content.

Another suspicious initiative that was forced on operators was a drill under the supervision of the IT organisation (ITO), another part of the ICT ministry, which was a drill to cut operators' access to root Domain Name Servers (DNS) that are an important part of the internet. The idea was presented to operators that SCVS wants to ensure if the West sanctions IRI and cuts its international links, access to local websites will not be impacted. Such initiatives made it hard, even for the optimists, to believe that NIN is not going to one day replace the internet for Iranians.

How does a network provider operate under the rule of IRI

What author has experienced

As stated before, IRI takes resources that are essential to any access network provider as hostages. A licensed operator has a legal obligation to comply with its license terms, conditions, and appendices. Two of these appendices of the licenses that CRA grants to network operators are the **Security Appendix** and the **Cultural Appendix**. How do these two appendices impact the work of a network provider that operates under the regulations of IRI?

According to its charter that is passed by the parliament of IRI, TIC is the exclusive provider of international links and inter-province links. As a B2B business, they have created a Customer Relation Management (CRM) platform to manage customer requests. When a network provider wants to expand its links (for example its international links that provide internet capacity), it must lodge an expansion request in TIC's CRM. TIC will attend to this request, only after the owners of security and cultural appendices approve the request. Without their approval, the network provider will be deprived of the resources such as internet links (provided exclusively by TIC) or radio spectrum (allocated by CRA). The network provider has a choice: Do not provide services or Comply with regulations to gain access to resources that are essential to providing services. Below is what the author has learnt about these two appendices:

- Security Appendix

  The authority that should confirm the compliance of the network provider with this appendix is a department in CRA that is named the “general department of the security of the communication systems”. While this department is under the organisation chart of the CRA (a part of the ICT ministry), its staff are said to be originally hired by the ministry of intelligence and seconded to serve in the ICT ministry.

- Cultural Appendix

  The authority that should confirm the compliance of the network provider with this appendix is a department in TIC that is named the deputy of cultural protection. Same as above, its staff are believed to be originally hired by the ministry of intelligence and seconded to serve in TIC whose chairman of the board is a deputy to the ICT minister.

Although the content of these appendices is kept confidential and is usually only seen and signed by the CEO of the network provider, the author of this submission can safely guess some of the obligations that are listed in these appendices from the experienced instances of failing to obtain the approvals that were necessary for expanding links from TIC or for the commercial launch of a new service or receiving a new allocation of the spectrum from CRA. Below is a list of such obligations that the network providers must comply with to launch new services or expand the existing ones

- Authentication of the registration data of all subscribers through an API gateway provided by the owner of the security appendix. The API gateway is named SHAHKAR and the process ensures the relevant authority knows who exactly is the user of each SIM card as well as other fields of information such as the residential address of the subscriber
- Ensuring the relevant authority has access to the database of all Call Detailed Records (CDR). These records are kept by network providers according to the standards of mobile technology to issue bills and settle disputes. However, the owner of the security appendix can use this data to discover which subscriber has made a call (or used another service) under which cell of the network at any certain date/time.
- Providing administrator access level on any new network node that the owner of the security appendix demands. This allows the relevant authority to run commands on the nodes without even informing the network provider. Such access must be granted before any live traffic is handled by the new node.
- Shutting down any service at any area upon the request of the owner of this appendix (i.e. the general department of the security of communication systems in CRA who in turn gets such commands from security-related authorities such as the Supreme Council on National Security, The Security Council of the Country (in the ministry of the interior affairs), The Securitisation Council of the Provinces and the like. These entities are predominantly concerned with the security of IRI and not that of the Iranian nation)
- Committing to three-party contracts with the owner of the appendix and its trusted contractor companies. The contractor companies must be paid by the network provider. The price is dictated by the owner of the appendix. The scope of work is agreed upon between the contractor and the owner of the appendix, and the contractor is responsible for delivering the platform that the owner of the appendix needs for interception or filtering. The network operator is only responsible for payment upon approval of each milestone by the owner of the appendix and until the final approval of these contracts is given by the owner of the appendix, the network provider must not hope to receive approvals on its

previously submitted TIC link expansion requests. More on this will be covered later in this submission.

- Providing space, and power, and facilitating access of those contractors to network provider's facilities such that they can install their platforms and connect the interfaces of their platforms to network nodes.

These contractors are local companies that are trusted by owners of the appendices to deliver platforms whose purpose is to carry out interception/filtering. Below is a list of such cases for various services:

- 3GPP standard interception

  To comply with the security appendix, the network provider must connect all new core network nodes' standard Lawful Interception (LI) interfaces to its Monitoring Centre (MC). The connectivity is described in relevant technical specifications of 3GPP which is the main standardisation body of mobile technologies. The trusted contractor of the authorities for these matters was a company named Zaeim Electronic Industries.

- Mass interception

  For IRI, standard interception is not enough as per the security appendix and the below services are under mass interception:

  - Internet

    The trusted contractor that does the job for the owner of the security appendix and must be paid by the network provider is Zaeim Electronic Industries. A local company that is said to be under full control of the technical department of the ministry of intelligence and delivers what is referred to as the data probe. They must be given their dedicated shelter in the network provider facilities and they hold the key to this shelter. The network provider must give them access to interfaces that aggregate the internet traffic to packet core nodes. Then they install optical splitters that take the aggregated traffic and split it into two identical streams. One stream goes the normal path to the network provider node and the other takes an identical copy of all the traffic to the platform that they have installed in their dedicated shelter. The platform will enable the owner of the security appendix to create IP Detailed Records (IPDR) and record which subscriber has accessed which destination IP address under which cell of the network at any certain date/time.

  - SMS

    Both for SMS filtering and SMS mass interception, all SMS traffic is routed to the box of the trusted contractor of the owner of the security appendix. In this case, the trusted contractor is a company named Peyk Asa. Each SMS takes only 140 bytes (before compression) and storage is affordable. This explains why many detained dissidents have reported that their interrogator had a copy of their SMS and intimidated them by pretending they know everything. The platform can filter certain SMS that contains a prohibited phrase and yet send a fake delivery report to the sender. Mass interception of SMS enables IRI to easily hack into people's OTT application accounts (such as WhatsApp, Telegram, etc) unless the subscriber has activated two-factor authentication

and chosen the second factor to be something other than a One-Time Password (OTP) that is sent to her phone via SMS.

- Voice

  The owner of the security appendix has a trusted contractor whose platform can start recording all calls in a certain area upon the request of the relevant authority (usually when there is a protest rally going on). The author is not aware of the name of the related trusted contractor.

- Signalling

  Towards the end of the author's days in Iran, the owner of the security appendix was pushing for another one of its trusted contractors named Oloum-e-Sabz. This contractor had a platform for mass interception of signalling links. This enables the authority to intercept events such as "location updates" and can potentially help them find the list of people in an area, albeit not always accurately.

In standard interception, you must have a known suspect and trace his mobile number with a judicial order. Mass interception enables the authorities to intercept all or a certain group (based on their location, a certain text message content or other factors).

To encourage Iranians to trust local OTT applications, the current minister of ICT has quoted a fatwa from Khamenei that says subscriber data should be kept safe such that people's privacy remains protected. Apparently, IRI has a radically different definition of protecting people's privacy.

- Internet Filtering

  As per the Cultural Appendix, the network provider must comply with the requirements of TIC's deputy of Cultural Protection. A fancy name for a department whose job is to filter internet content.
  As per the author's experience, several authorities can command certain content to be filtered. One is the "Committee for Identification of the Delinquent Content". But even someone in an inspector role in the judicial branch of IRI can command certain content to be filtered (this was how Telegram got filtered in Iran). Upon such command from authorities, a chain of events happens.
  The owner of the cultural appendix (TIC's deputy of cultural protection) commands its trusted contractor to execute the requested filtering policy. The platforms that carry out the command are separated into two layers. The higher layer is a managerial platform that registers the requested filtering policy and ensures proper performance criteria are met by platforms in the lower layer. The higher layer platform that does the managerial tasks is provided by a company named Samaneh Gostar Sahahb Pardaz which is one the trusted contractors that work for the owners of the appendix. The lower layer platforms that enforce the policy (i.e., perform the Deep Packet Inspection (DPI) and block the content or throttle down its speed, whichever is commanded by the upper layer platform) are provided by two other trusted contractors: "Dadehpardazan Douran" and "Yaftar Pajouhan Pishtaz Rayanesh". These platforms have shown the ability to block different content (including VPNs) or slow them down. That is how most VPNs are not properly functioning whenever IRI authorities want. Of course, no technical platform is flawless and there is always a race between those who wish to block people's access and those who want to help them against the blockade. The fact that some videos of the recent uprising have made it out of Iran is

more a sign of the limited shortcomings of those platforms rather than proof for IRI to claim that it has not meant to block people's access. The platforms that enforce the filtering policy are said to be capable of enforcing smart filtering. The author speculates that by smart, they mean the platforms can enforce different policies for different subscribers or based on certain geographic areas or other such attributes. This requires the boxes to sit between the packet core nodes of the network provider and the firewall that sat between their network and TIC. Authorities were pushing network providers to implement this architecture in late 2019.

- Throttling internet bandwidth
  As mentioned earlier, often the authorities delay the expansion of the internet links that the network provider must lease from TIC to push for compliance with their ever-increasing requirements. This creates congestion and lowers the speed of users. Also, since all the traffic must go through the filtering boxes, the performance of those boxes can significantly impact the user experience. The long list of requirements of IRI authorities degrades what Iranians experience when they access the internet. Even on calm days. Even for the non-filtered content.
  Apart from this, because of its exclusivity, TIC can decrease the internet bandwidth that it has allocated to any network provider to slow down the internet for users. If authorities command that, TIC which is a part of the ICT ministry will obey.

The author had experienced how in 2019, the authorities were pushing for "smart filtering" as well as a solution that enabled them to conveniently shut down any service that they wanted at any time they wanted over any area that they wanted. Although they could utilise their unrestricted access to network nodes to do this, and operators had to comply with the terms of the appendices and shut down their services upon their request, the authorities wanted to have something far more user-friendly and without any need for any cooperation of the network providers. Ideally, they wanted to draw a shape on a map and with a few clicks, shut down certain services of all operators in that area at once. The author speculates that these matters were part of the aforementioned item 38 of the NIN master plan (The execution of the master plan of the Control Appendix under the framework of the Security Appendix of the NIN).

What the author has learned from reliable sources

- Post-2019, IRI authorities have managed to get ready for the implementation of "smart filtering", at least so much as the network architecture of the filtering boxes is concerned. Upon implementation, they can enforce different filtering policies for different subscribers. Rightfully, many see this as dividing society into classes with different levels of privilege. If IRI trusts you, you can access the internet. If not, you may only access the intranet.
- Although IRI has many tools to intercept and filter, they seem to have convinced or more likely coerced all websites and applications in Iran to provide them with access to their servers and logs. This makes it dangerous for the Iranian dissidents who use these services. There are numerous reports that people have been located and arrested after the authorities have traced them using the record of their activities on these websites.

- Most Iranians must use VPNs to access common destinations on the internet because the list of filtered content has grown very long. There have been cases where free (or even paid) VPN services are provided to people just to monitor them. The user assumed that the VPN server is under the control of some foreign entity, only to realise later, that the VPN server, which would know all the details of the subscriber activities, was controlled by IRI and used to intercept its users.
- Both Google and Apple application stores have blocked certain Iranian applications for malicious behaviour. This suggests that IRI has been using some local applications as spyware that sits on the user's phone and has access to a lot of user data. This can provide IRI with much more than what they could get from intercepting the networks.
- During the recent uprising, on some days, IRI has used internet curfew by stopping traffic on TIC links that provide internet to access network providers (a.k.a. operators). Also, it has severely decreased the international bandwidth that it had previously allocated to the operators. There have also been instances reported by users that not just the internet, but all other services were shut down in areas of unrest.

Conclusion

IRI claims in submission #19 (Additional Information2) are far from reality. By abusing its power and taking essential resources hostage, IRI has deprived the Iranian nation of accessing telecommunication services for years. After years of holding Iranian telecommunication networks behind, IRI only permitted network expansions as a means to build its desired NIN. All along, IRI maintained its hostage-taking tactic to ensure its tight digital grip and restrict Iranians' access to network services, especially the internet. The width and breadth of tools that IRI uses to restrict, intercept, and cut services of Iranians show how they interpret the privacy-related fatwas that they are so proudly referring to. The only way to make sense of IRI claims is to consider that by "nation" they mean the minority that might still be supporting them. By "National" security, IRI means its survival at the cost of taking an overwhelming majority of Iranians hostage and depriving them of their basic human rights. Had ISIS been recognised by the international community as the legitimate state of Iraq and Syria, it could have used similar excuses to justify its brutal digital crackdown.