In the High Court of Leidi

Criminal Appeal No. 108/2011

Appellant: ***1. Mensi Industrial technology Corp (MIT) represented by Mr. Smith & 10 others***

2. TinySmooth Inc. (TS) represented by Mr. Anderson & 5 others

vs.

Respondent: ***State***

1. HARBHAT is a fast developing country that had obtained its independence in 1947 from the British through various peaceful and non-violent movements. It has a huge population next only to China. The youth ratio of Harbhat is a healthy 60%. The Capital city of Harbhat is Leidi.

2. In the past decade, Harbhat witnessed a fantastic growth in its economy that was an eyesore to many nations. Even during the current depression, Harbhat was the least affected.

3. To meet its huge requirement of energy, Harbhat looked into alternative clean energy generation, especially nuclear power generation, besides wind and solar power. Technology and industrial development in many spheres had and continue to have an element of foreign country's vital presence in one form or the other in hardware, software, and know-how. To protect its information technology and security techniques, Harbhat adopted 'The International Standard IS/ISO/IEC 27001' and periodically adapted its upgrade.

4. Harbhat is a defacto nuclear power and not a signatory to NPT. But the world powers, though recognized its peaceful nuclear programmes, had been pressurizing it to sign NPT and put obstacles in its quest for import of Uranium for its reactors.

5. Though Harbhat had a small nuclear arsenal, it has a very strict policy of no first strike and had its delivery routine highly secured. Through its various actions, on very volatile situations, Harbhat showed extraordinary maturity, and did not rattle its nuclear saber. Very often this attitude was criticized as being too docile, by its own citizens. But this was appreciated by many nuclear powers despite their differences.

6. Harbhat had its own Uranium mines though of a very insignificant capacity. But it had a considerable deposit of Thorium, on which it has done good research and exploring opportunity to exploit this resource for its power generation.

7. Harbhat, indigenously and also through collaborations, has established itself as world class in the field of automobiles, medicine, space exploration, software and many other fields due to its large percentage of young intelligent human resource. Many of its young citizens are technically highly qualified and most chose to do higher education in top technical schools throughout the world. A very high percentage of the exceptional students after completing their research have occupied key positions in the reputed research facilities, in nuclear physics, space exploration, medicine, biotech, robotics etc.

8. Harbhat recognizing its growth stimulus and grand plan gave a clarion call to its citizens settled abroad to return and serve the nation in its growth and help achieve equal position among the developed nations, which is its due for a long time.

9. This call had a favorable effect on the young minds, who had the same feeling to somehow give to the nation what they have received from it.

10. The top policy makers discussed among themselves the priority to be accorded to the programs of its future development. They identified that the power generation for its upcoming industry is the foremost challenge, given the rise in the price of oil and the non reliability of sources like solar and wind energy.

11. Harbhat decided to augment its nuclear energy production and decided to construct nuclear reactors for enrichment of Uranium for the power generation. It entered into various agreements with different developed nations for the construction of nuclear power plants. However, the attempt on part of Harbhat to enter into these agreements was sought to be blocked by some of the other nuclear powered nations, both, out of animosity as well as out of a concern for use of enriched Uranium for non-peaceful purposes. It was also widely reported that several fundamentalist outfits gave media statements threatening dire consequences for Harbhat, with regard to the proposed nuclear reactors.

12. During the agreements, issues related to Harbhat's nuclear weapons program surfaced. Harbhat was categorical in its reply, that their nuclear arsenal is strictly for its defense purpose, considering its hostile neighbors. The raw material for this purpose is not in any way connected with the dealings with its partners. All activities in this regard from raw material to technology and knowhow of Harbhat are indigenous. Though its partners were skeptical about it, they could not do much about it.

13. Ukusa the most developed nation in the world, exerted pressure on Harbhat to sign NPT and created various hurdles in its acquiring technology, knowhow from other developed nations by pressurizing them not to export high end technology which may have dual purpose and objectives.

14. Harbhat was in long time association with TinySmooth Inc. (TS). TS is a Multinational Corporation and delivered software solutions to a number of enterprises in virtually every field. Its servers were ubiquitous. Their varied operating systems spanned personal, industrial and technological arenas. They also had specialized solutions for robotic assembly line control, industrial applications for various advanced instruments and machinery, specially operated by servers called Program Logic Controllers (PLC).

15. PLCs are high ended programs that control the operations of various industrial applications automatically and do not depend on any human intervention. The supervisors only needed to keep an eye on the parameters at regular intervals, to identify any changes or fluctuations, which is nearly non existent, since PLC takes control of all such changes and issues appropriate warnings or direct the instruments / machinery to appropriately adopt to the changes, keeping in mind the strict output requirements, within permissible limits. In essence they keep the functioning of the various instruments, operated by the highly sensitive and powerful motors strictly under control in tune with already programmed output parameters.

16. Mensi Industrial Technology Corp (MIT) is top industrial conglomerate and has its wings spread in the entire world. They are giants in the field of manufacturing and supplying Industrial machinery for practically every purpose. They also manufactured prototypes based on research models given by nation states. Mensi's main industrial production is in Mercala. Mercala is a developed nation and highly industrial in nature. Mercala is a G5 and Security Council member and is in close association with UKUSA in keeping a watch on the activities of the world.

17. Mensi had production units throughout the world and had a very advanced unit in Ukusa. Due to the global market depression, Mensi also faced problems to maintain its organizations and keep intact its technical personnel who come at a very high cost.

18. Mensi had its production units in Harbhat also. But mainly they were of machinery, due to the availability of raw material in plenty. The Industrial Control Systems were manufactured either in Ukusa or in Mercala and imported into the countries and establishments where Mensi's products are installed. Mensi's products are used in various industrial establishments like, turbines, water treatment plants, power generation, chemicals, traffic lights management systems and nuclear power generation systems.

19. Harbhat uses Mensi systems for many of its industries that include public and private enterprises. Some of the enterprises are world class and their products are used world wide. Mensi Industrial Control Systems, that perform the critical work of modern life, are also used in food industry, fertilizer production units, pharmaceutical industries where chemicals are mixed, dams, reactors and also in biotechnology industry for the centrifuges. They are also used in the space programs, the operations of which are kept confidential.

20. In Harbhat on July 21, 2010 one of the centrifuges in a biochemical factory went bust due to erratic spinning. It did not attract much attention and was promptly replaced.

21. During the same time, in September 2010, Resby Security Systems of Ontario, who are experts in protecting Industrial Control Systems (ICS) from digital incursions that can sabotage installations, received many enquiries on their website looking for information about ICS. Resby's flagship product *Torino*, a security suit was specified for this purpose. This was unusual, as the information is very specialized and the seekers were not from the regular users. The IP addresses revealed that many of them were from EROM, a nation in the Middle East. The users wanted very specific details on Mensi's PLC-720, which is a large ICS, which also happens to control the speed/spinning of uranium enriching turbines.

22. This fact was interesting as this was the time when there was a lot of news circulating about a worm 'StunNet' hitting industrial systems. Major Anti-Virus protection agency Sytstematix also revealed that 'StunNet is an extremely rare variety of worm whose exact nature is a mystery'. An ingenious mapping technique adopted by Systematix revealed a strange geographical pattern of the infection. Out of 40,000 infections in that given period, 25,000 infections were from one country, EROM, alone. Harbhat had 7000 infections and Ukusa had a few infections viz., about 700 during the said period.

23. Subsequently in Nov 2010, Mahud Jada, President of EROM issued a notification, that enemies of EROM have tried to sabotage their nuclear facilities which suffered a limited setback that have been rectified and they are back into work. In Jan 2011 when IAEA completed its inspection at Zatan in Erom, they found that something was unusual with their centrifuges. The normal replacements would be about 10-15% i.e. 800 centrifuges in a year were now in thousands, close to 3000 – 4000 replacements.

24. On Jan 15 2011, The Ukusa Times (UKT) reported that the StunNet was a very sophisticated cyber weapon that only a few nation states have the capacity to build and deploy. The scariest thing about StunNet is that the people who wrote it had capabilities that most other people did not have. The quality of the code was military grade. UKT charged that Ukusa and Lasri were behind it. It was a known fact that both these countries, Ukusa and Lasri, were very vocal against the nuclear programs of EROM right from the very beginning.

25. The most striking aspect of StunNet is that it used about four Zeroday exploits which is considered to be extremely rare even among professional malware creators. Although this was new in itself as control systems aren't a traditional hacker target, because there is no obvious financial gain in hacking them. What StunNet did to the systems was apparently not new. The most unsettling thing about StunNet was that its components immediately hid themselves on entering into the host. It appeared to be simply stealing configuration and design data from the systems, presumably to allow a competitor to duplicate a factory's production layout. StunNet looked like just another case of industrial espionage, its malicious intentions ingeniously masked.

26. Though the public story that the virus is spread through USB stick, experts did not believe that was the only way. The most enigmatic feature being that the systems that were infected were not connected to the web. StunNet had different ways to spread and the most important aspect was that it was aimed at infecting Mensi's ICS which are deployed to control large assembly lines to nuclear power plants. For those systems that did not use Mensi's ICS, the virus was inert.

27. Worried by the news of the specific infection target of StunNet, Harbhat scientists and technicians incharge of the nuclear and other sensitive installations, thoroughly checked the correctness of the system operations.

28. With available details put forth by Anti-Virus companies and experts and also with in house experts, it was seen that few of the systems at Harbhat was also infected and some of the centrifuges were not doing their task perfectly as expected. Besides the technical loss, the looming threat of a nuclear meltdown due to imperfection of the final product, which could not be gauged due to the camouflaging of the results / reports in the monitors and output medium, was a serious matter in hand. The officials of the nuclear facility was not sure whether an accident at the facility a month back when one of the technicians was injured seriously and later succumbed was due to this.

29. Meanwhile the StunNet worm details were available on the Internet. Experts warned that since specific details were available, it would be easy to replicate by hackers community and would cause havoc to Industrial / defense / research establishments throughout the world. A senior nuclear physicist of Russia, who did not wish to be named, warned that if EROM goes ahead with its program with the present developments, its Uranium Enrichment reactors would most likely face a meltdown, which would be at least 50 times more disastrous than Chernobyl.

30. Perturbed by the news, the Prime Minister of Harbhat issued a strong statement on March 14, 2011 saying that any attack on Harbhat or its facilities in any domain will be retaliated in the strongest terms and that the cabinet was meeting with the head of all the chief political parties with the specific purpose of enacting a law to consider treating "cyber attacks an act of war" in the ensuing session of the Parliament. Prior to that he would recommend to the President to issue an ordinance forthwith to the effect.

31. Subsequently with the recommendation of the council of ministers and leaders of the political party, the President of Harbhat issued the 'Harbhat National Cyber Security Plan' ordinance on April 12, 2011(see annexure for salient provisions) .The major provisions outlined were in essence similar to that of Ukusa – Comprehensive National Cyber Security Initiative.

32. A thorough enquiry was ordered by the Prime Minister of Harbhat. On enquiry, it was found that a tourist who was later identified as Mr. Ramesis from Ukusa was seen in the neighborhood of one of the facilities. The doubts were further compounded when he was also seen in a restaurant at the adjacent table where one of the technicians of the facility was dining with family. For a brief moment there were images in a frame in the CCTV, Mr. Ramesis was seen talking to the children of the technician and handing over a CD which was later identified as music RW CD. Further investigation

led to the details that Mr. Ramesis was found in the same foyer of a musical concert, where an official of Mensi was also present.

33. Dr. Ragnar, cyber security expert from Mercala, who is also a specialist in PLCs, gave the following interview in a reputed technology magazine TekSpeak. “Very few hackers could manage four zero-day vulnerabilities and two stolen certificates, and even fewer would waste all that on one worm. This is what makes it "unprecedented", not the quality of the code and went on further to state, “Supposedly it has never been seen in the wild. It is highly likely it wasn't when the system was designed but might have been added after to help with fault diagnosis. As such the engineering companies (Who are?) who put in the plants and commissioned them would have been involved in this potential attack as a source of the electrical design drawings although their complicity would be unknown. Find these companies and check their electrical engineering people and you'll uncover if they willingly helped.”

34. On 1 Sep 2011, the Special Investigation Team, after detailed investigation, enquiries took into custody Mr. Smith, CEO of Mensi Industrial Technology Corp along with 10 technicians and Mr. Anderson, CEO and Chief Technical Head of Harbhat of TinySmooth Inc. along with 5 other technicians and produced before the Sessions Court of Leidi on the following charges

    1. Mr. Smith, CEO, Mensi Industrial Technology Corp and all other technicians 1 – 10 of Mensi – under Sections – 108A, 121 & 121 A, of HPC and Sections 43, 43A, 65, 66, 66B, 66C, 66D & 66F of Information Technology Act 2000 as amended by HTAA 2006/08, read with Sec. 120B of the HPC.

    2. Mr. Anderson, CEO & Chief Technical Officer, TinySmooth of Harbhat and all other technicians 1 – 5 of TinySmooth – under Sections – 108A,121 & 121 A of HPC and Sections 43, 43A, 65, 66, 66B, 66C, 66D & 66F of Information Technology Act 2000 as amended by HTAA 2006/08, read with Sec. 120B of the HPC.

35. After an elaborate trial, the Sessions Judge pronounced its judgment, and held them to be guilty of the charges, and convicted all the accused. Media reports were live with the arbitrary use of Sec. 120B. The Sessions Judge convicted and sentenced all the accused to Life Imprisonment citing the grave danger to the lives of the vast population of Harbhat and the unimaginable damage it would create for the atmosphere as a whole.

36. The accused persons have appealed to the High Court of Leidi against the judgment and order of the Sessions Court, on all counts.

The participants are free to raise relevant issues, technical and legal. The laws of Harbhat are similar to that of India. The participants may logically presume / assume facts that are based on recent events.

Annexure

Harbhat National Cyber Security Plan (NCS Plan)

Purpose and objective

Cyberspace will be considered an operational domain like land, sea, air and space. That military has to operate and defend its networks and prepare for cyber missions and cyber conflict.

Section 5

A Special Investigation Team (SIT) headed by a Commissioner, who will be of cabinet rank, be constituted to enquire matters related to NCS Plan who will be under the direct supervision of the Prime Minister of Harbhat.

Section 6

5 point provisions

1. Cyberspace is considered an operational domain like land, sea, air and space
2. Defense Ministry will improve cyber security and develop new defense operating concepts and computing architectures
3. Defense Ministry would partner with other government departments and agencies as well as the private sector to enable a cyber security strategy that encompasses the whole of government
4. Strengthening of ties with allies and international partners to enhance collective cybersecurity
5. Engage creative / innovative minds through an exceptional cyber workforce and rapid technological innovation.