Crowley Presents :

New computer controlled systems, or full network layouts for exploitation by Millennium's End Hackers.

Networks :

- Medical network
- Scientific/Laboratory network
- Travel agency
- Bank
- Amusement park
- Airport
- Software House

Computer controlled systems :

- Oil tanker
- Cruise ship
- Oil/Gas platform
- CCTV
- Submarine
- Military Analysis, Command and Control system.

The first section is computer net layouts for normal use with the hacking rules in ME, however, some of these may not be accessible via the GenNet, and may have to be accessed using other dial up connections.

For effective access to some of these systems, creation of a Communications skill or subskill might be required, especially for use of satellite and radio communications and system links.

The second group is not really layouts, but will be presented in their context of being connected to company/organisation networks, i.e. The Oil tanker control system will be a subnet of the Oil company's normal setup. The second group is my favourite, since they are relatively simple to visualise, and can give some interesting plot hooks. For some sort of idea of what could happen; Oil Tanker (Hackers, or the series Stark), Cruise Ship (Speed II, Deep Rising). Think of the possibilities of taking over, or influencing the movement of a Submarine! Other uses of these plot hooks are to have another faction hack into them, and the Cell's job is to return control to the correct authorities, etc, etc, etc.

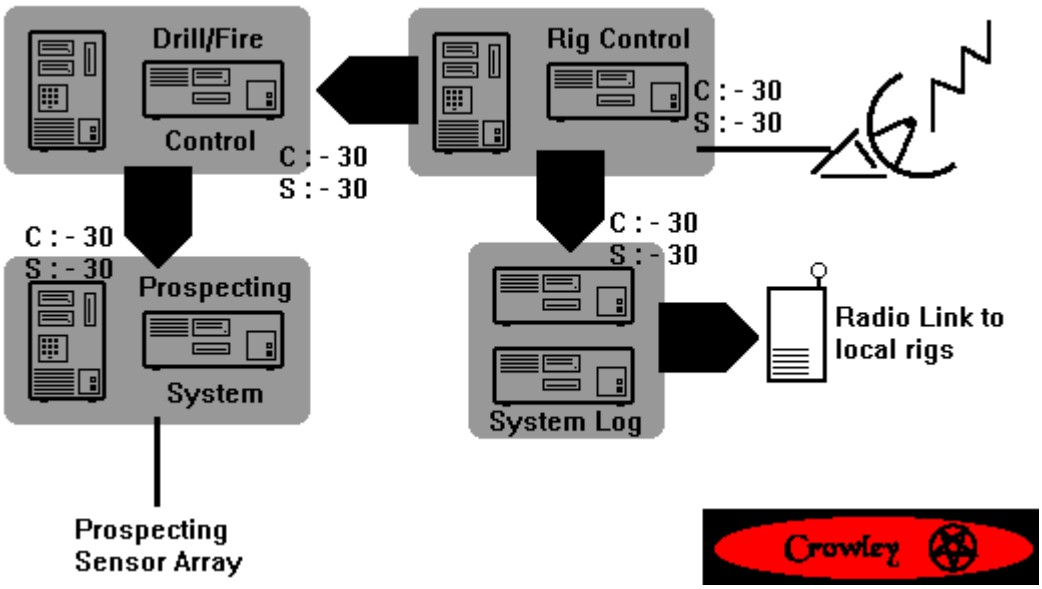
The final entry on the list is "Military analysis and control system" quite a few years ago, in a scientific journal (we're talking about 1983 ish here) I read about the development of system designed to disseminate information around a battlefield, most of these have become a reality now, but there is still a lot of automation still possible, and this is the area which I'll write up into a system layout, it might be a bit sketchy, but there should be enough to get a GM going if he finds a cell trying to go into one of these increasingly complex and controlled systems. This sort of system could ultimately lead to a battlefield with no actual living soldiers on it, simply a computer controlled network of artillery, tanks, and even air cover. The exact reasons for a having a cell try and hack one of these are a little hard to define, but some GMs might like the extra background and principles. Any cell involved in, or near a conflict involving a highly developed nation's military might encounter these.
I have to give credit to "Insight" magazine, and the Centre for Information Warfare research, reachable at www.terrorism.com. I know this sounds a little far-fetched, especially the human free battlefield, but the general principles are quite sound.

Oil Rig computer system.

This is, like most of the computer-controlled systems being described, a fairly simple network, run by a main control console (Rig Control). The main entry into this system is by remote satellite link from the corporations main operations section (not described, for Corporation Nets, see the ME GM's handbook). The main rig control operates the basic functions of the rig, if it is a manned rig, the accommodation environmental controls, lift and emergency systems. It also carries out the rigs navigation if it is an independently powered rig capable of movement. It stores all operations in a main system log which records all activity on the rig. The rigs Drill/Fire control operates the fire emergency systems, and administrates the Drilling system (on automated rigs) which actually carries out the drilling for oil/gas. These types of automated rig are really only practical in shallow waters, as drilling at any depth usually involves a lot more maintenance not possible without human intervention. This system is linked to a sophisticated prospecting system using a large underwater sensor array which in conjunction with research material and/or a systematic drilling strategy can find smaller oil fields which would cost too much to exploit with full manned rigs..

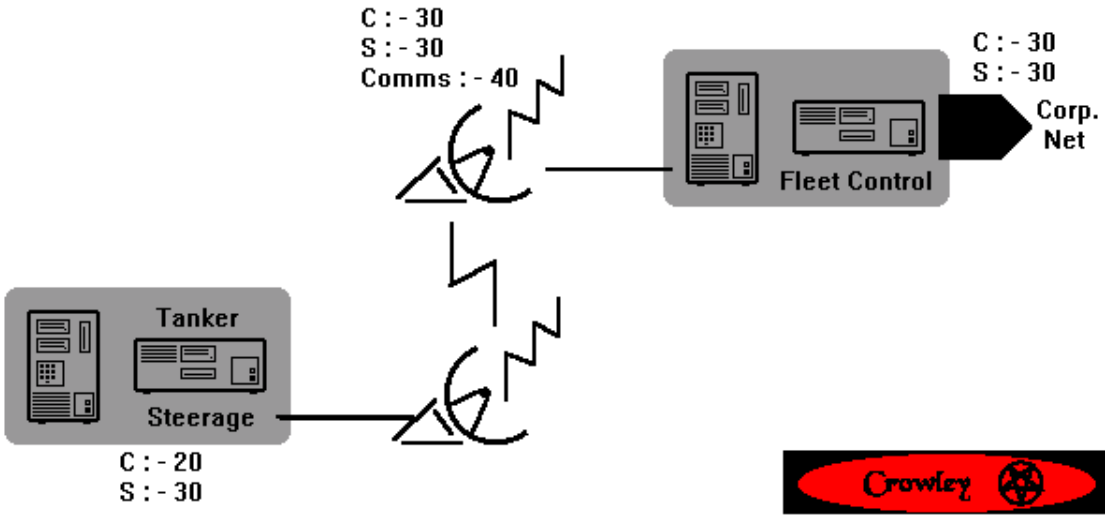
The last item to describe is the Radio link, which makes the rig itself a node of a small network of rigs, both manned and unmanned, this is for the purpose of using several unmanned rigs to exploit large areas of sea, and to keep manned rigs in basic communication with each other for safety reasons. This radio network is another route that a hacker may exploit.

This network may be fun if the corporation is running a large group of unmanned rigs, especially if these are only being used for prospecting, and not full oil production. Unmanned rigs could fulfil a variety of functions, as most are still fitted with rudimentary accommodation and power facilities, with short term food supplies, along with a helicopter pad, and communication facilities. A fairly secure base of operations could be run from one with very little interference from outside, especially if the actual operations of the rig are not interfered with. And as maintenance crews only visit the rig every 3 weeks or so, anyone there would not be noticed for a while.



Oil Tanker control system.

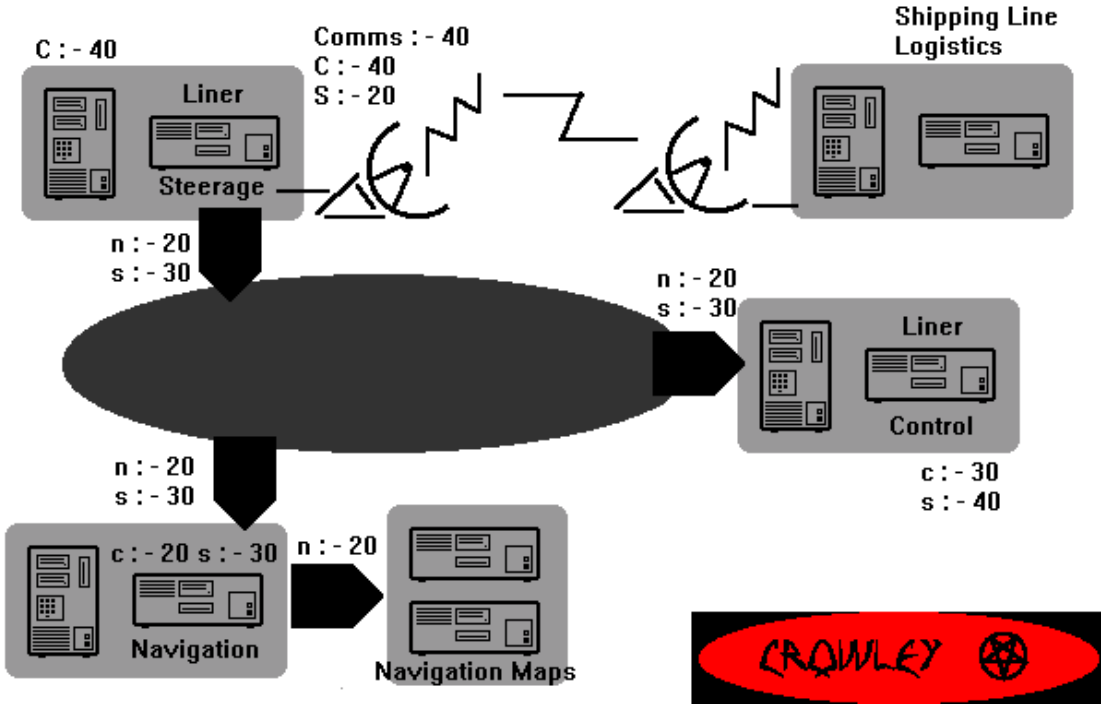
This system is even more basic that that of the rig, used primarily for navigation of large tankers without a human crew, essentially this is one computer based control linked to the companies net by satellite link. Used alongside automated rigs, this could provide a company with an almost completely automated oil production and transport system. This would only be used with rigs exploiting small oil fields where pipelines would be impractical. In some cases the GM may decide that a completely unmanned tanker may be unlikely, however, in the same way as the rig, these could provide inexpensive transport for a cell if they could take control of the navigation system. The GM may want to seed an adventure with the hijacking of a tanker's control system by either pirates who sell on the oil, or by a rival oil company. This system also controls the tanker's emergency controls, including a radio beacon for location purposes, and the emergency dump controls which could eject the tankers contents into the sea. Both of these would need security unlock codes which would only be held by the company, and may need manual entry into the on-board console to work. The tanker would also come with a heli-pad for a work team to board it in transit.



Cruise Liner.

These computer controlled systems are leaning towards automated control of transport systems, or large vehicles. The main reason for this is the small amount of personnel involved in running these systems (navigational and authority personnel) can cost large amounts of personnel, and most of the time they are fairly specialist, and as such, specialists are more easy to replace by intelligent computer systems.

This network is similar to the Oil Tanker's, but a lot larger to reflect the variety of functions it needs to take care of. In the same way as the Tanker, it takes control of the navigation system, controlling the ships travel (a great adventure seed, check out "Deep Rising", this came out after I'd written this, but shows what could happen…;-), but it connects to a larger, more conventional network, to link to the Liner control system. This is the meatier part of the system, which is basically similar to a building control system, it controls bulkhead doors, lift systems, environmental controls, lighting, even down to running the film in the liner cinema. In the even of an emergency, it controls the emergency radio beacon, and can be set to deploy lifeboats and to release them when they reach capacity. This is one system which can never be completely unmanned, but requires less skilled personnel, such as navigators, and can allow far more freedom of movement to the ship, and more flexibility of travel. Some engineering and electrical repair personnel will be carried as standard for engine repairs etc, and at least one computer technician fully qualified in the system, and its application to navigating a cruise liner (ie not just any old network tech)

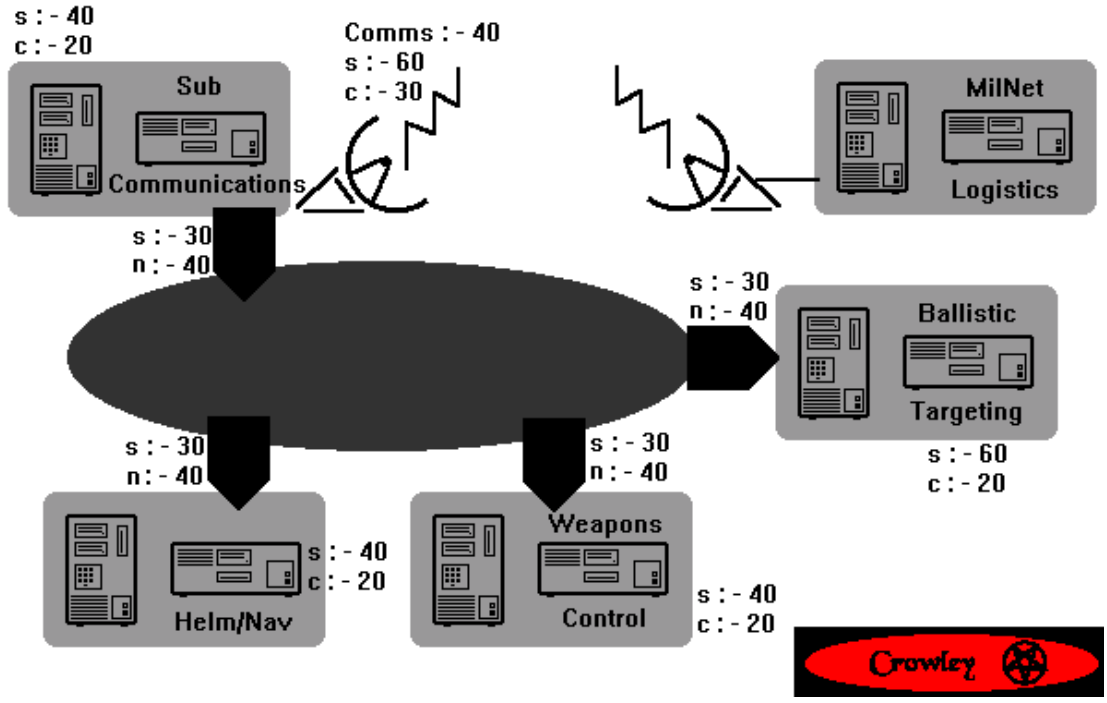


Military Systems

The last two systems I'll describe here I've kept together, as they both patch onto the Milnet system I wrote for the sourcebook part 1. The first is an extension of the Tanker/Liner vehicle control systems, but instead of a ship, I've gone underwater and described the automated control system for a military submarine. I think of this as going a bit too far towards the Shadowrun/CP2020 style of having the matrix/net overshadow everything else, but I'm still putting it in, coz the layout is fairly sensible, and realistic, and if a country decided to automate these things, then this would probably be pretty close.

The main starting point I suppose, is the MilNet logistics system, I put this on the original MilNet layout in part 1 of the sourcebook, but considering what it actually allows the hacker to do in this case, make the modifiers for getting into that system a *lot* more difficult. This connects via satellite, to the Submarines main network, the Sub communications system distributes control messages around the network, and to any personnel included on the Sub. The first is the Helm and Navigation system, this basically controls the travel of the sub, this may use the Sat uplink for Global Positioning.

The other 2 control systems included on the diagram are potentially the most fun/dangerous/unbalancing to the game. Firstly is the Weapons control, this controls the Subs locally offensive weapons systems, sonar targeting, and torpedoes. When surfaced, the Sub may include some local artillery, and surface to air missiles. For special operations the Sub may also be fitted with underwater mine laying gear. All of these weapons are controlled by this system. The Ballistic targeting system is only included on Submarines equipped with a long range nuclear capability. GMs may modify this to be harder to breach, although to get this far, the hacker will have had to cross a multitude of barriers of the MilNet system, the Satellite link, and then hack through to this system. This system is capable of passing targeting info to the missiles being carried by the Sub, to actually fire them requires a seriously large code key, which would require 45 minutes to break, and a security roll at -80. Bearing in mind that any access to the MilNet system will usually mean triggering a trace program, this means that any attempt to break this and do anything would be highly dangerous. A GM may argue that for any missiles to be actually fired would require a manual entry at the Targeting console, this makes a lot of sense, but with control of the Helm/Nav system, one could steal a nuclear armed sub which could be a lot of fun. Please note though, any use of brute force entry of one code after another is ill advised, as some systems are set to automatically disarm the missiles after 3 incorrect code entries, requiring manual reset by qualified personnel. All these little snags mean that you might be able to fiddle with the sub, and maybe move it around, but you wont be firing off nuclear missiles left right and centre. Although just the control is a pretty scary thing when you consider these sub carry Surface to air missiles, and a full complement of torpedoes.

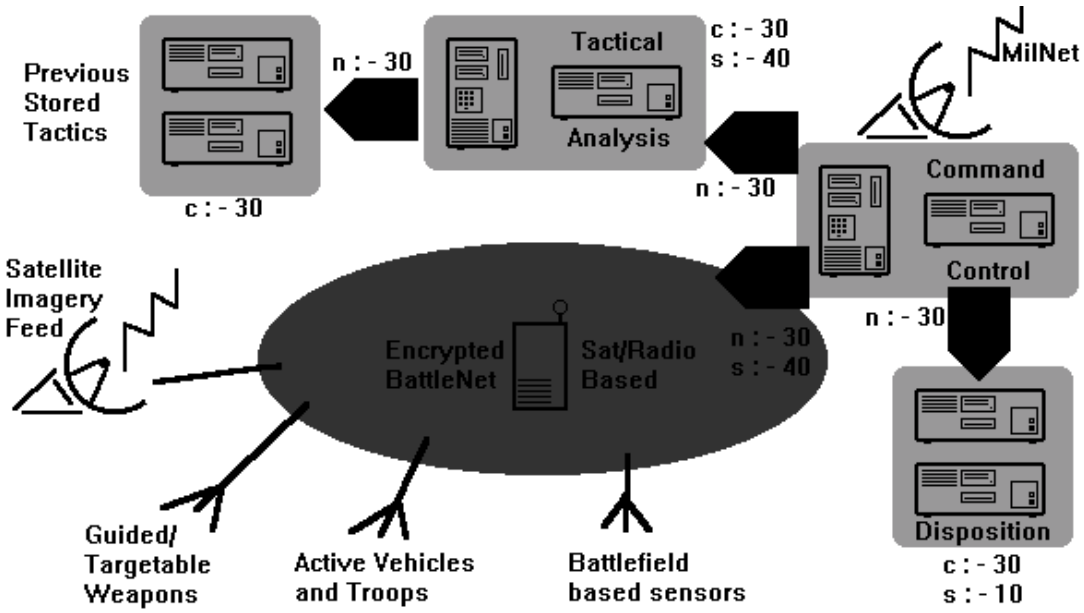


Electronic Battlefield Environment.

This is one of the more interesting systems I have considered. This came out of an article from a science journal called “Insight” published in the early 80s in the UK, it was a Tomorrows World type magazine covering all sciences, including Military technology. The article discussed the dissemination of battlefield information to and from the soldiers on the ground, to tanks and artillery for targeting purposes, and to battlefield HQ, this covers most reasonable scales of battlefield, from Sea going tactics, large scale land offensives, down to a few acres of muddy field somewhere in the former Yugoslavian territories.

Ultimately, the system transmits summaries back to MilNet, so there is a satellite uplink to connect to this, the Command control is the central point of the network, being manned by experienced military commanders who can direct the battle from behind the scenes. This uses a large data store to keep track of the position of all Electronic Battlefield (EB) equipped units. On top of this, there is a large “Wargames” style battle simulation system, used to test and predict various battlefield strategies before they are committed to aid the officers in charge. This computer is also used to pass targeting information from spotter units to artillery and other pertinent data to and from units in the field who require it. There will usually be a real time satellite image feed from satellites overlooking the area, to add to the information being passed from the field to build as complete a map as possible for the Command Control to look at. EB units will be equipped with a variety of systems, including laser targeting systems, GPS units, and portable computers to give them an independence of movement, and they will all be carrying encrypted digital transmitters to ensure a secure network.

This layout would only be really useful if the players are in a conflict in which this system is being used, they may be asked to compromise an enemy’s system, or may find it to their advantage to infiltrate a friendly network to pass information into it, or retrieve information for their own use. A very good programmer might even be able to influence the results of a combat simulation to push the battle in a certain direction. To compromise the main encrypted radio network will take a communications roll at -40, and a security roll at -50. This may take up to half an hour to complete, and if both sides are using an EB system, expect there to be Information Warfare specialists on both sides trying to compromise each others system.



CCTV system

CCTV systems are taking over, there's no doubt about that, Big Brother is truly here to stay. So, as an operative, you probably want to stay on top of the situation, especially if the Op you're on is on the darker side of the law. This could probably be modified for both city centre monitoring, and even Motorway surveillance. Using this system, it would probably be possible to track a person through a city centre without the need for a shadow on the ground depending on the level of surveillance you require. The CCTV system has a Main Storage system. This comprises a large Server, with Re-Writable Optical disk recorders, each capable of storing about 2 hours worth of footage from one camera, or up to four cameras at reduced resolution. There is an automated loading system to replace the disk at the end of each 2 hour slot, and the disks are re-used every 3 days. The CCTV cameras themselves are remotely controlled, with zoom functions, Low light, Infra Red, and under good lighting conditions give crisp, clear footage. The whole system is controlled from the Control Station computer, which is usually manned, but can be left unattended for up to a week if necessary. If it is unmanned, it is possible to use a dial in connection to take control. The lobby computer is used to monitor and control cameras that are too far away from the Control Station to be hardwired in, such as remote sites where a manned station is unfeasible.