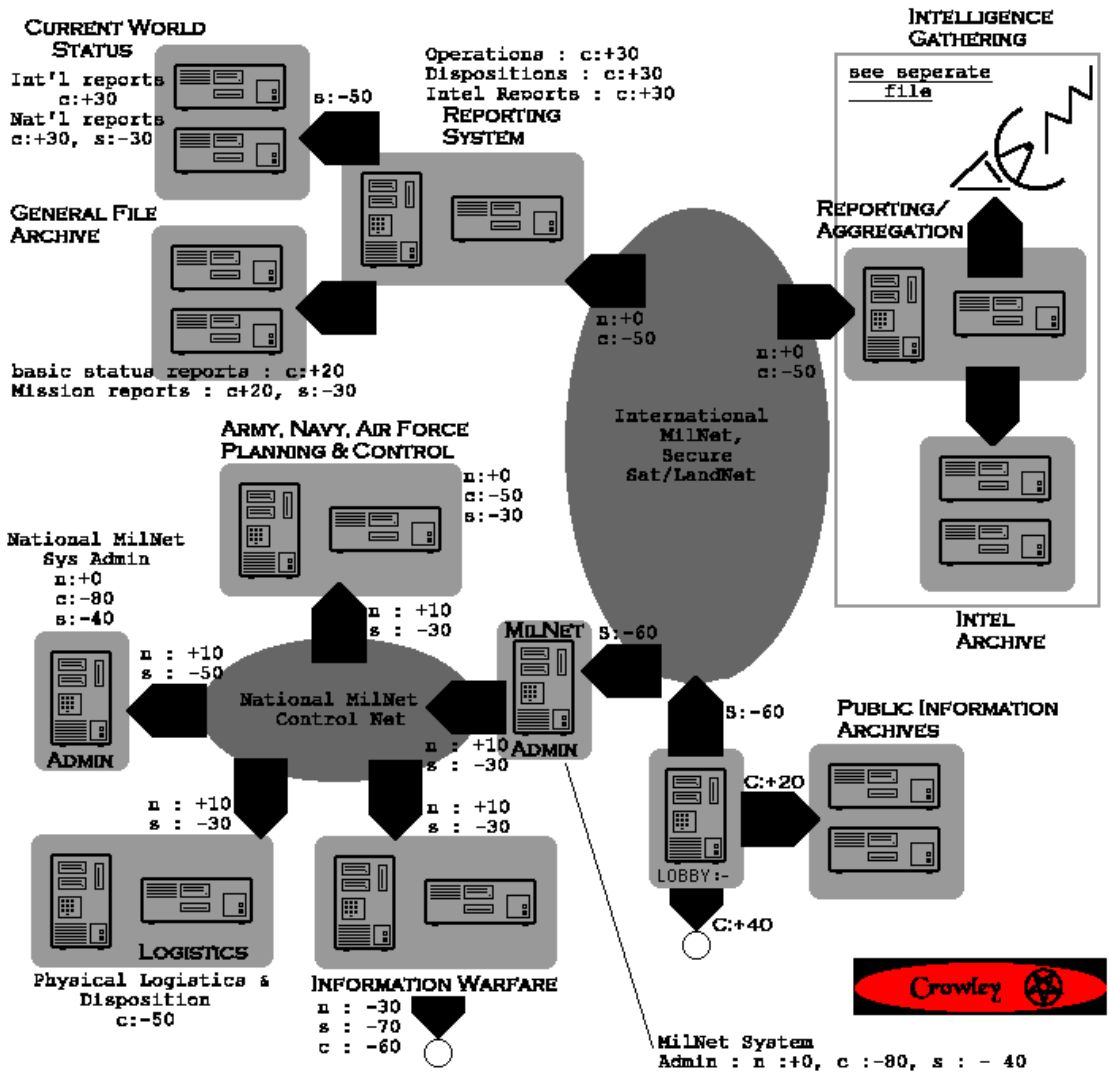
MilNet System, with Notes.

OK, for starters, a few words on this layout.

- I know absolutely sod all about military systems, I'm just making up what I think would be a well structured system in terms of systems design and security issues.
- the US has a MilNet, probably on a much vaster scale than this, I'm lumping sections together to make a (relatively) simple, system layout, anything more, and it gets too big for simple use in an ME game. The US MilNet also has gateways accessible through the Internet, I don't know why, the security holes that exist in it must be phenomenal, it's a wonder we don't hear about more break-ins than we do (wonder why?). As far as I know, the UK and most European countries operate their own military networks, but as they are more centralised (smaller geographical areas to cover) they are mostly on private encrypted, scrambled or just plain physically different phone lines and physical networks.
- I purposely avoided things like "Nuclear Deterrent Control Centre". ME operatives accessing this sort of stuff is simply too stupid for words, besides, in the ME world, after Gulf II/WWIII, this stuff is likely to be impossible to get into, and probably on a completely different circuit.
- Its big enough to have some juicy servers to hack into, but small enough to hack through in, say, half an hour of game time.
- Of course, if anyone wants to hack into India's Nuke research system, let me know, I'll spin one off in no time (hardly any security, primitive third world country (WISHFUL THINKING))



This is the basic system layout, the Intel section is covered later on in this document.

The main Grey subnet in the top right, is an international accessible network, secure from the GenNet due to the use of completely separate and enclosed communications network. Ways of getting in through this network are also discussed later on.

Lobby, and Public Info.

The first section to describe is the Lobby and Public Information Archive. This is a simple reporting system, with public access information. This might include Public Relations material, recruitment adverts, and even some declassified reports and documents. The lower civil systems bonus is to reflect the sheer volume of data, and the difficulty of finding what you want in a short space of time.

Reporting System (top left on the diagram)

This is the MilNet's main reporting system, containing concise reports and files on the worlds status. This is not to be confused with the Intel Section's reporting system, this holds a lot less detail, with a lot more generalisation and more analysis and supposition on subjects. Think of this as the reporting system for the top brass, low on detail, but high on consequences and suggestions for further development. The **File Archive** holds these reports, dating back usually up to the last 4 years. Anything older than that will be on hardcopy, and physical backups, not accessible by the hacker.

The **World Status** system holds sorted information on political and military matters around the world, again, it contains less detail than the Intel Archive, but holds a lot of additional material by analysts, suggesting consequences, or extrapolations from the reports held on the system. (note, the lack of detail difference between this and the Intel archive could be items like the codenames of missions performed to get the intel, and items like agent identities etc. this dort of detail is irrelevant in this level of reporting.

The **Reporting System** itself, acts as the update, and search system, much as the Agg/Rep system in the intel section.

MilNet Admin.

This is simply the cut-out between the MilNet itself, and the central MilNet system. If you want to visualise it, think of the MiNet as the National network, and the Central MilNet as the Pentagon. This system regulates the use of the national network, accessing this will not let you get into the Intel Sections Archive server, but it *will* let you get into the Intel Section itself, and into the Reporting System itself with a lot less bother. However, if you can control the Central control Admin, this gives you control of the whole system both networks, and all connected computers. Of course, you still have to break into it first……unless you can control this system you will not be able to access the Central Control network.

Logistics.

This is fairly dull, but the odd nugget of useful info might come in handy, if you want to re-direct some equipment your way for example. This contains information on the physical disposition of all military personnel, and equipment in the world under the military's control. Troop positions, supply line information, plans for upcoming troop movements, and transfers, stock levels of everything from fuel, ammo, right down to soap, and where these stocks are. With the right organisation, a cell could possibly redirect supplies (small amounts), or alter stock levels while they walk off with the difference.

Central MilNet Admin.

The real biggy. If you can get into this, you have control over the whole thing, that's why :

- Its hard to get into
- its the other side of some heavy security already (place the admin furthest away from the GenNet gateway)
- It has lots of those nasty little toys on from the GenNet sourcebook.

Army, Navy and Air Force Planning and Control.

Possibly boring, possibly very interesting indeed. This system has information on the basic policy, and strategy of each of the main Military branches (make up one of these servers for each of them if you want). Dates of upcoming intelligence and military missions, strategies being employed against certain countries, information on coalitions, shared information and intelligence. This has all those miscellaneous bits of info, fleshing out the big picture.

Information Warfare Section.

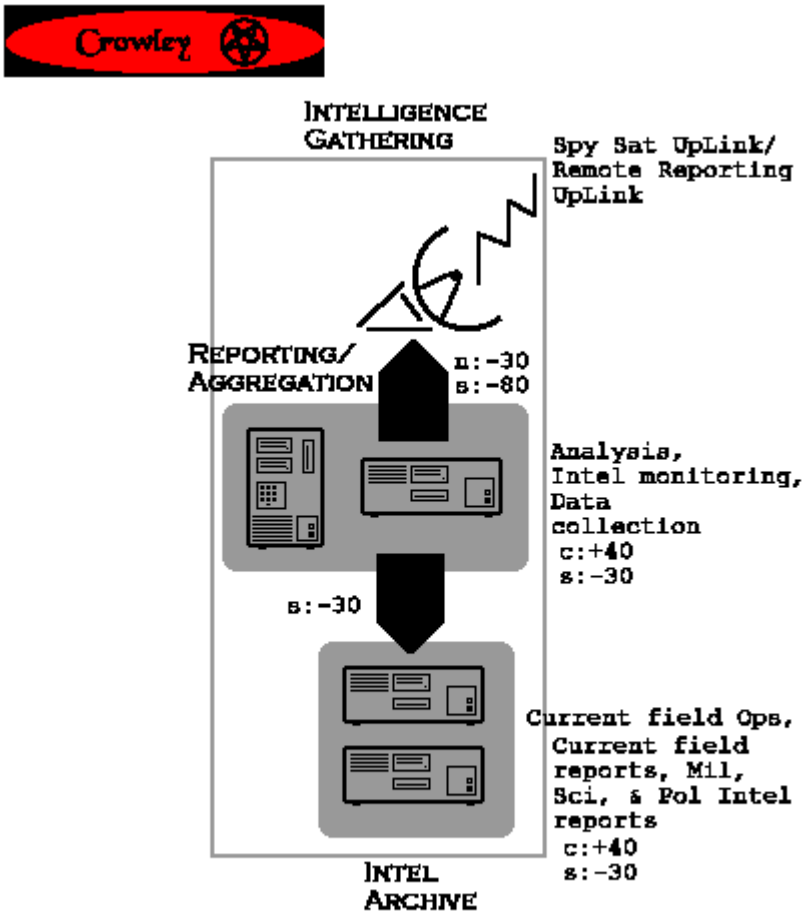
The most tricky area to look at. This section is essentially staffed by 2 groups of people, Hackers, and Psychologists. Information warfare, is warfare carried out using the flow of information. This flow of information can be defined in several ways :

- Public information, newspapers, television, general propaganda
- Communications systems, phone systems, radio, satellite, computer networks
- False intelligence reporting to the target

This section contains information about all of the above, any hacker getting into this system is taking a very big risk, first of all, they are very likely to be traced, and/or attacked using a Crash or Flash program (see GenNet sourcebook), and if they are traced, physical retribution, or being busted by the FBI is soon to follow.

Files on missions, and operations designed to destroy an enemies communications, and propaganda operations and tactics being used on an enemy are likely to be found here.

There is a GenNet gateway from this section, however, it is unlisted, and is likely to change, maybe even leading to dead-ends, and false addresses. This is the Military hacker's connection, from which they are likely to attack other systems, and to develop their own hacking skills. Some of these hackers are likely to work behind codenames and handles, and may even be known to BlackEagle hackers by these names, and depending on the request, may even aid a BE/BE hacker, depending on the ethics of an operation. They may use this anonymity to spy on hackers, and their operations if they interfere with Government operations or organisations. Then again, Military hackers may even operate solo, just like other hackers, using their own resources, and working alongside normal hackers. Military personnel are very secretive, and their identities are very, very difficult to discover, nevertheless, these identities may be held somewhere on the MilNet system…….



When I was designing this net, I thought it might be a good idea to break this section off from the rest, as it has a fairly specific role to play, and it involves the Sat uplink, not described in the rulebooks.

Uplink.

The use of this is fairly obvious, it facilitates the reporting from the field by agents, and by units, of their status, and intelligence.

Reporting System.

The Reporting/Aggregation system, sorts, files, and links together intelligence reports. This sounds simple, but the constant flow of data may well contradict other reports, and/or update current information. Several pieces of intel may arrive on the same subject, but from different sources, the aggregation system merges all of these bits on info together to form a coherent file of intelligence on a particular subject. The Intel archive is simply the library that the aggregation/reporting system uses for long term storage, this frees up the rep/agg systems space for immediate and important use.

Archive.

The Archive holds a current, up to date record of live field operations, be they agents on solo missions, or satellite reconnaissance, or units on live or practice missions. Alongside this, it contains political and high level espionage reports, on the state of countries finances, and operations. This is why it is kept on a branch of the system, which is very difficult to access.

There are 3 ways of getting into this section of the MilNet,

1. Hack in, using the basic route, from the GenNet connection of the MilNet, then into the Intel section.
2. Hack into the MilNet admin, and use the control of the system this gives you to go straight through the Intel security.
3. use the satellite uplink to run a signal into the MilNet Intelligence archive, this may give you limited control of the rep/agg system, as access is given on an area by area basis. Logins and passwords refer directly to live operations, any requests for information not directly pertaining to these missions is refused. In absence of a Communications subskill, this would take an electronics roll at -30, a civil systems roll at -30 and a security roll at -40. If someone comes up with a comms subskill, then this would be at -20, with a civil systems at -20, and a security at -40.

Once into the Intel system, a civil systems roll at -30 is required to access a report on a certain subject, and this is with a known password.

- Without a login and password for a certain operation, a security roll at -60 will be needed.
- A security roll at -80 and civil roll at -50 would get the hacker a list of operations with their logins.
- This wouldn't include the passwords, but once the login is known, the password can be bypassed by a security roll at -40.

Optional rules for the MilNet system.

If you're using the GenNet sourcebook, put a lot of toys into this one, Trace programs, Crash, and even Flash programs may be lurking on this one. This is a Military Network, don't show any hesitation in putting nasty things on this one, this is the network most (sensible) hackers stay well away from !

For countries other than the US, UK, and Russia, feel free to modify these rolls to make it easier for a hacker to get in, it all depends how hard you want it to be for a hacker to get into this sort of system.