USS SEA TIGER
NCC-2009
MARINE'S HANDBOOK

Stardate 0/2102.06
(06 Feb 2021)
UNCLASSIFIED

THE
Marine's Handbook
for members of
the
333RD Military Intelligence Group
"Yellowjackets"

USS Sea Tiger
NCC-2009

This manual is published by and for the USS Sea Tiger, NCC-2009.

Published Feb 2021

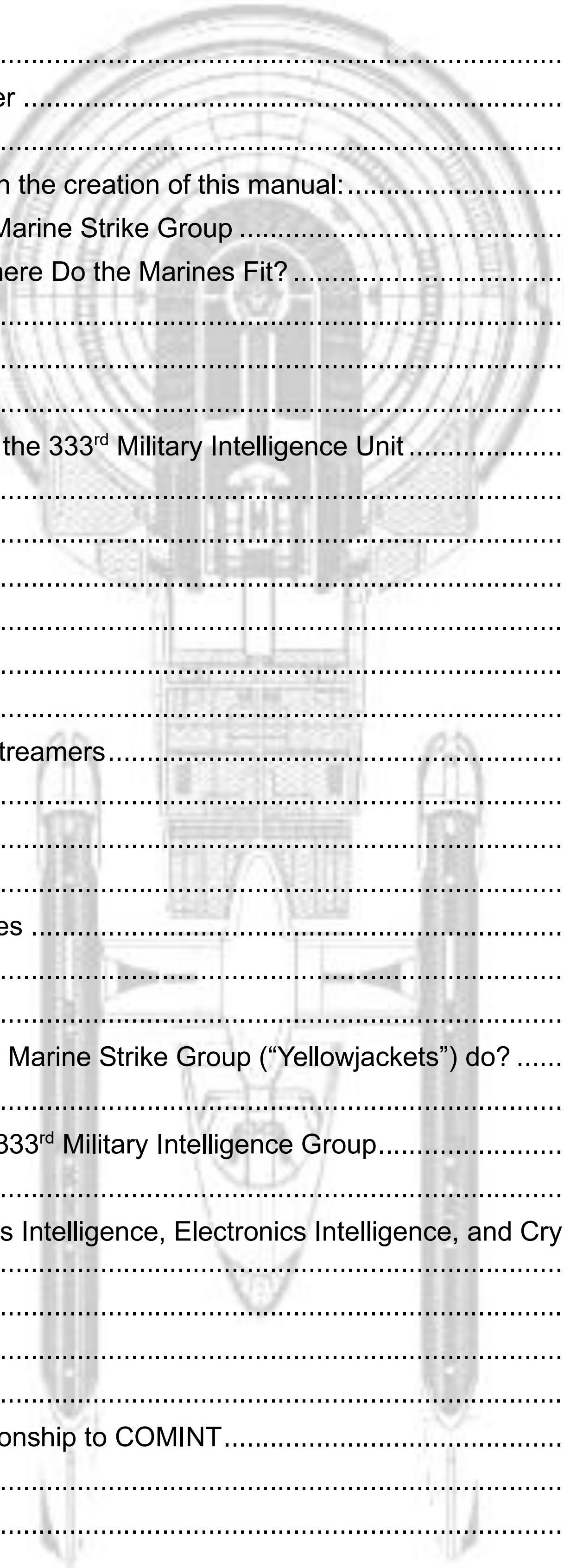
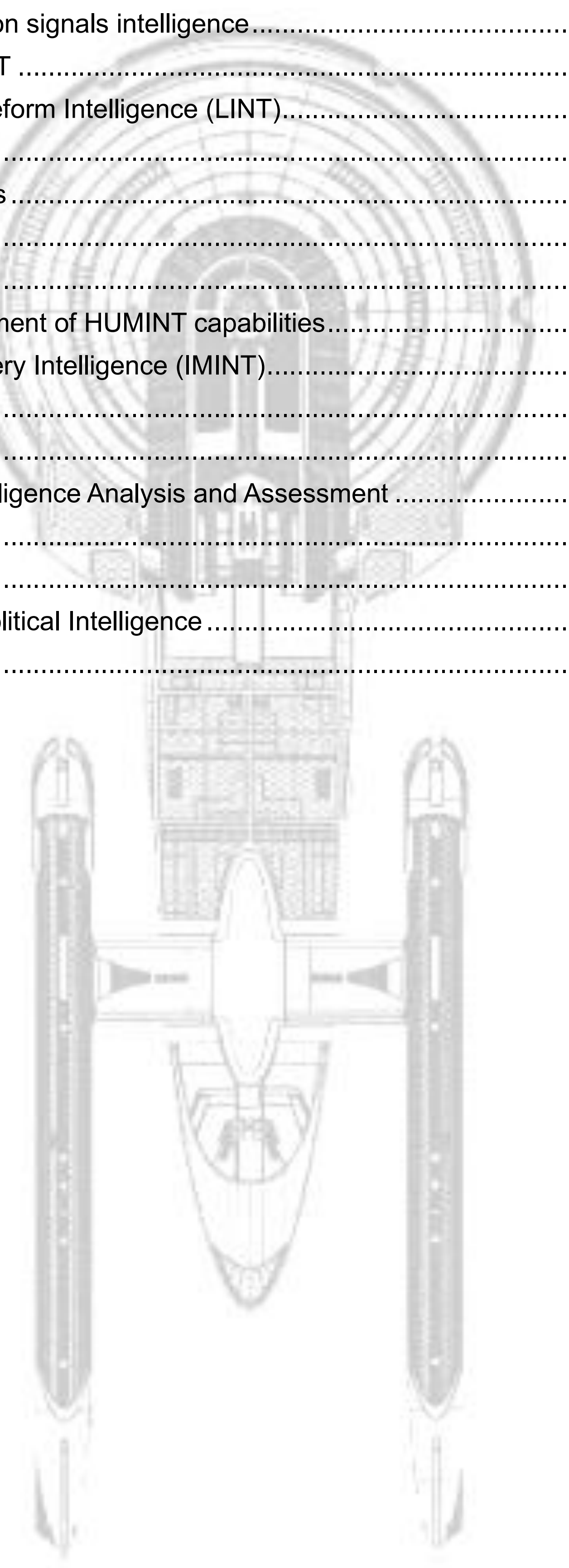
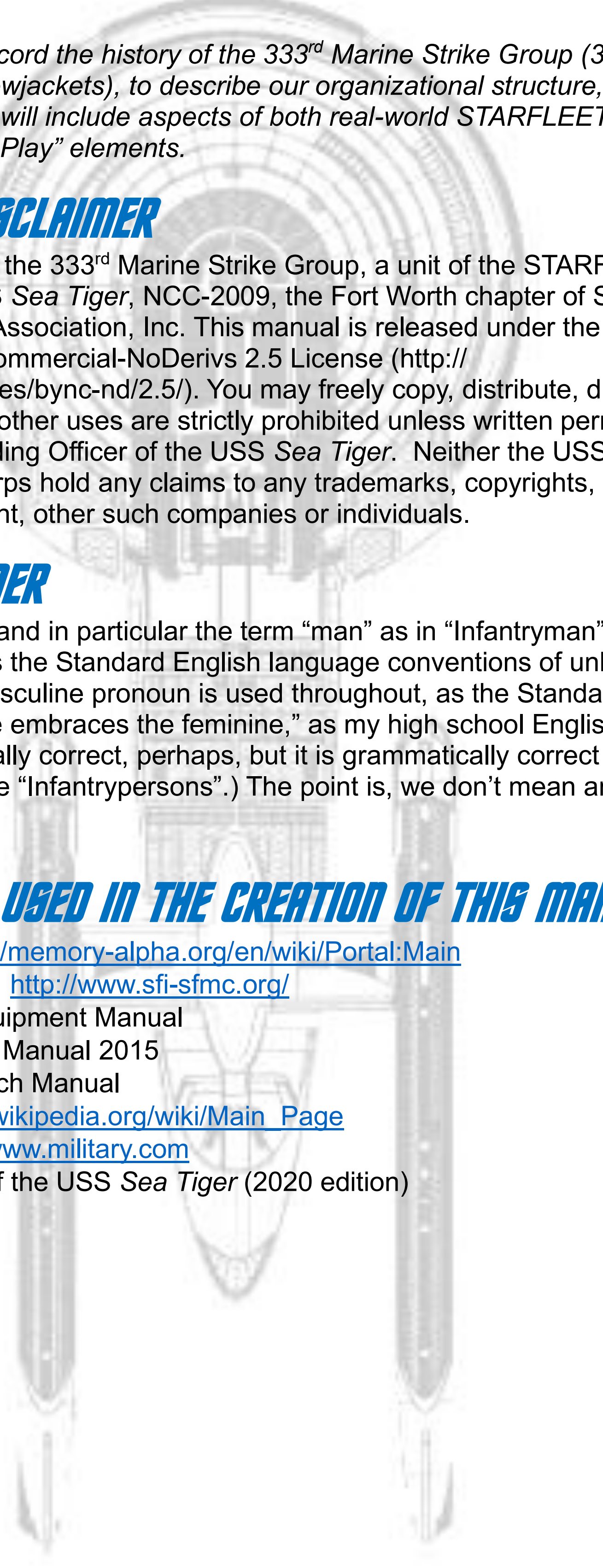


Table of Contents





Purpose

This guidebook serves to record the history of the 333rd Marine Strike Group (333rd Military Intelligence Group, the Yellowjackets), to describe our organizational structure, and to discuss operating procedures. This will include aspects of both real-world STARFLEET Marine Corps activities and fictional “Role-Play” elements.

Copyright and Disclaimer

This manual is published by the 333rd Marine Strike Group, a unit of the STARFLEET Marine Corps and a part of the USS *Sea Tiger*, NCC-2009, the Fort Worth chapter of STARFLEET, the International Star Trek Fan Association, Inc. This manual is released under the Creative Commons Attribution-NonCommercial-NoDerivs 2.5 License (http://creativecommons.org/licenses/bync-nd/2.5/). You may freely copy, distribute, display, and perform this manual, but all other uses are strictly prohibited unless written permission is received from the Commanding Officer of the USS *Sea Tiger*. Neither the USS *Sea Tiger* nor the STARFLEET Marine Corps hold any claims to any trademarks, copyrights, or other properties held by Paramount, other such companies or individuals.

Pronoun Disclaimer

The use of he/his/him, etc., and in particular the term “man” as in “Infantryman” or “crewman”, are used for convenience as the Standard English language conventions of unknown-gender pronouns. Likewise, the masculine pronoun is used throughout, as the Standard English convention. (“The masculine embraces the feminine,” as my high school English teacher always said.) It may not very politically correct, perhaps, but it is grammatically correct (and much less awkward than silly words like “Infantrypersons”.) The point is, we don’t mean anything by it.

Reference works used in the creation of this manual:

- Memory Alpha, http://memory-alpha.org/en/wiki/Portal:Main
- The SFMC Web site, http://www.sfi-sfmc.org/
- SFMC Arms and Equipment Manual
- SFMC Marine Force Manual 2015
- SFMC Support Branch Manual
- Wikipedia, http://en.wikipedia.org/wiki/Main_Page
- Military.Com, http://www.military.com
- The Ship's Articles of the USS *Sea Tiger* (2020 edition)

1.0 The USS Sea Tiger's Marine Strike Group

1.1 Ship's Structure: Where Do the Marines Fit?

As seen in the USS *Sea Tiger's* Ship's Articles (*The Chapter Handbook, General Orders, and Ship's Constitution of the USS* Sea Tiger*, NCC-2009*), the ship has three Divisions: Gold, Red, and Blue. All members of the ship, except for the Captain and First Officer, belong to one of those three Divisions. Each Division has a different real-world area of responsibility – for example, the Red Division is responsible for Recruiting and Retention.

There are three other organizations on board the *Sea Tiger*, that are not departments but in many ways act like them. These are the 333rd Marine Strike Group (The "Yellowjackets", the 333rd Military Intelligence Group) a unit of the Third Brigade in the STARFLEET Marines Corps; the *Sea Tiger's* Klingons, and the 33rd STARFLEET Rangers ("The Paladins"), a unit in STARFLEET Strategic Operations.

The USS *Sea Tiger* has more than one type of membership, and does not require a member of the ship to be a member of STARFLEET, The International Star Trek Fan Association, Inc. (STARFLEET.) He may, if he so wishes, be merely a member of just the chapter. These "Local Members" may serve in any department (other than the Command department), and participate in any ship's activity or meeting. He may be promoted as any other member of the ship, subject to the guidelines found in Article VI of the Ship's Constitution. However, membership in the STARFLEET Marine Corps (SFMC) and in the STARFLEET Special Operations (SFSO) are limited to members in good standing with STARFLEET. Therefore, to be a member of the 333rd Marine Strike Group, you must be a paid member of STARFLEET.

1.2 Authorizing Entities

There are two authorities for the USS *Sea Tiger's* Marine Strike Group. First, the chapter authorized the formation of the team: see the Ship's Articles, Article IV, Section 4.02(e). Secondly, the SFMC is the STARFLEET authority for all SFMC units, including ours.

According to the Sea Tiger's Ship's Articles, Article IV, Section 4.02 (e): "There will be a detachment of Marines on the USS Sea Tiger. They will maintain their own ranking and order of command where it pertains to Marine business. However, if a situation involves crew members who are not Marines then it becomes a matter for the Command Staff. Marines will receive the same respect and privileges as anyone else on the Sea Tiger as they are STARFLEET members who merely prefer a more military aspect to their role playing. Any International member of the USS Sea Tiger may become either an Active Duty Marine or a Reserve Marine at his own discretion."

1.3 Description

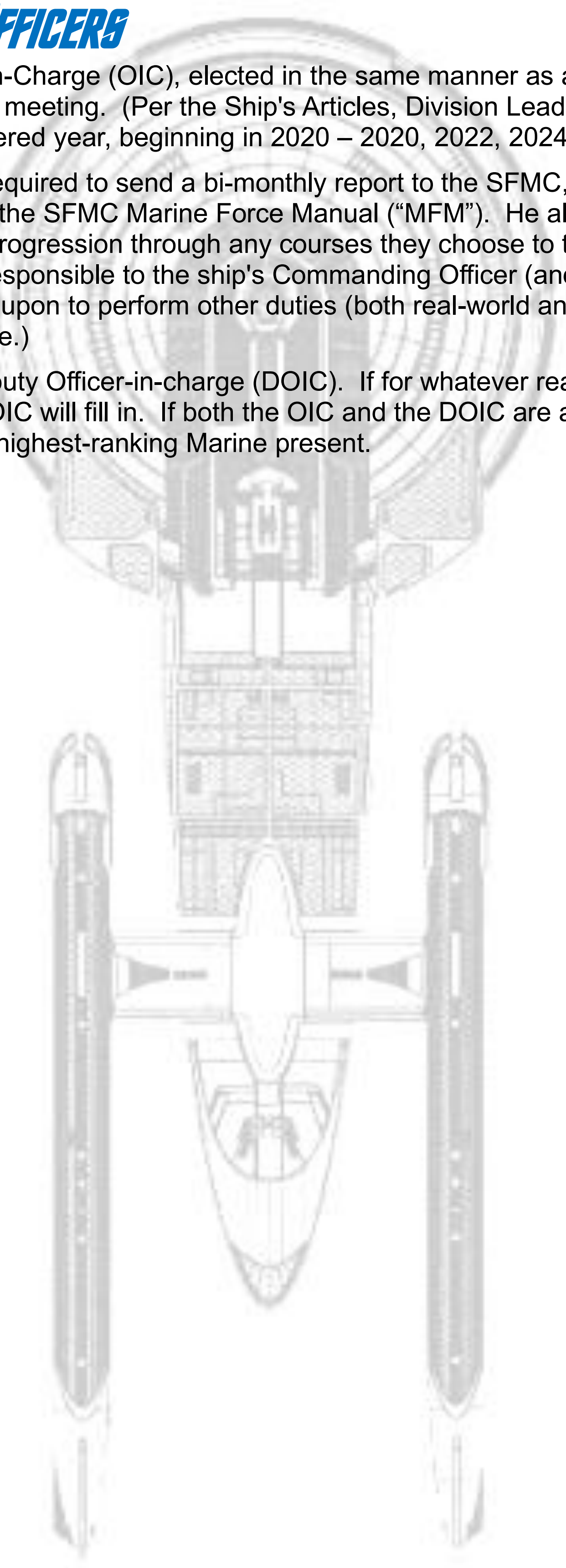
As the USS *Sea Tiger* is in Region 3, the 333rd Marine Strike Group (MSG) is an active part of the Third Brigade of the STARFLEET Marine Corps (SFMC). The unit is currently organized as a Military Intelligence Group, and members of the 333rd are encouraged to take SU-100 (Support Branch Basic Course), SU-201 Support Advanced Course, and SU-250 Military Intelligence Course from the SFMC Academy (SFMC-A) Staff College School of Support, as well as courses in the Institute of Intelligence & Espionage at STARFLEET Academy.

1.4 Duties of Officers

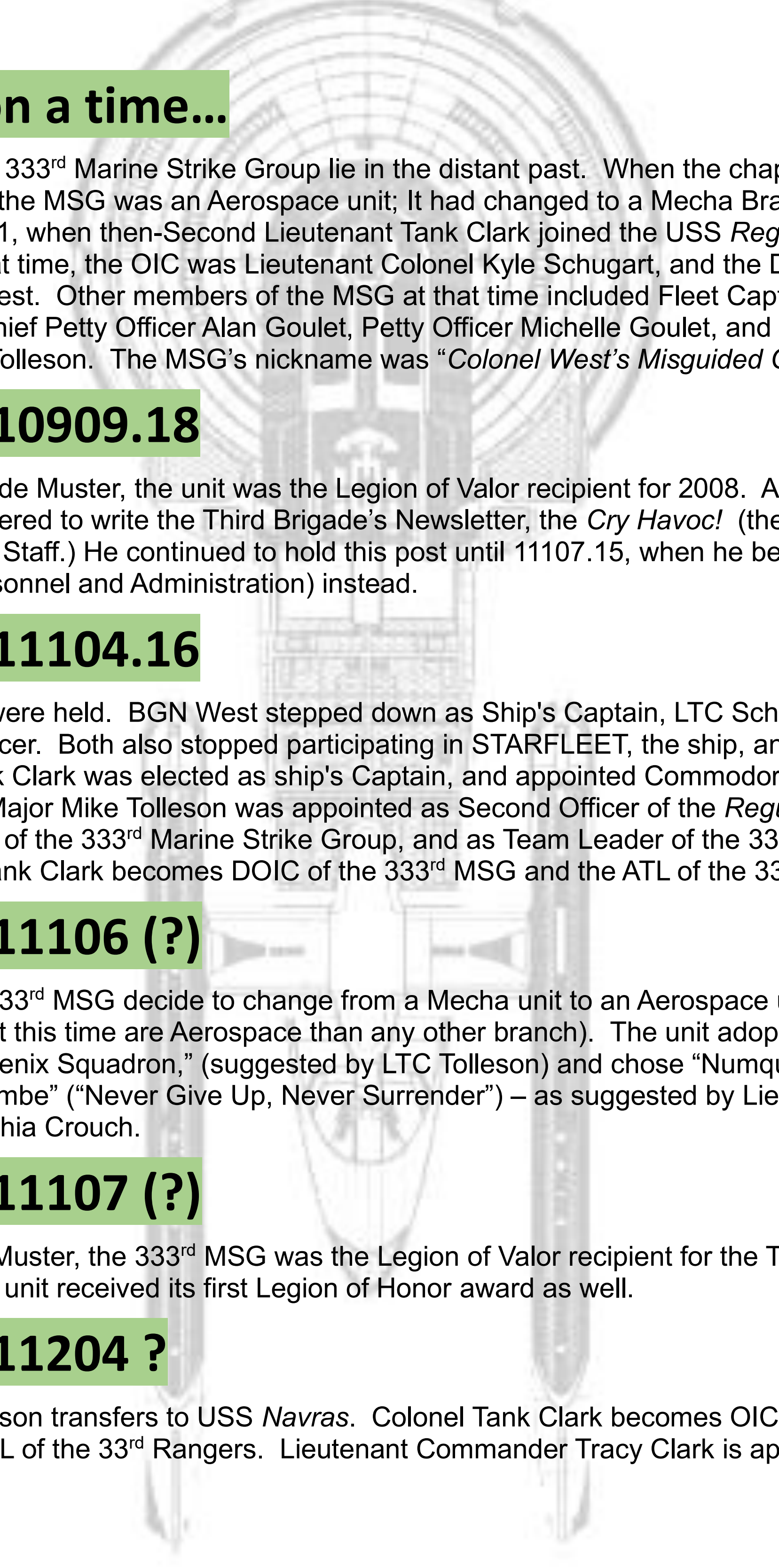
The unit has an Officer-In-Charge (OIC), elected in the same manner as a Division Leader, and during the same Election meeting. (Per the Ship's Articles, Division Leader elections are held in April of each even-numbered year, beginning in 2020 – 2020, 2022, 2024, etc.)

The OIC of the MSG is required to send a bi-monthly report to the SFMC, using procedures as set forth by the SFMC in the SFMC Marine Force Manual (“MFM”). He also assists all members of the squadron in their progression through any courses they choose to take at the SFMC-A. Additionally, the OIC is responsible to the ship's Commanding Officer (and other command staff), and may be called upon to perform other duties (both real-world and within the ship's fictional 'roleplay' universe.)

The MSG also has a Deputy Officer-in-charge (DOIC). If for whatever reason the OIC is unable to fulfill his duties, the DOIC will fill in. If both the OIC and the DOIC are absent, command of the team resolves to the highest-ranking Marine present.



2.0 Abbreviated History of the 333rd Military Intelligence Unit



Once upon a time…

The origins of the 333rd Marine Strike Group lie in the distant past. When the chapter was the USS *Comanche*, the MSG was an Aerospace unit; It had changed to a Mecha Branch unit by Stardate 10908.01, when then-Second Lieutenant Tank Clark joined the USS *Regulator* and the 333rd MSG. At that time, the OIC was Lieutenant Colonel Kyle Schugart, and the DOIC was Brigadier Mark West. Other members of the MSG at that time included Fleet Captain Liz Goulet, Master Chief Petty Officer Alan Goulet, Petty Officer Michelle Goulet, and Second Lieutenant Mike Tolleson. The MSG's nickname was "*Colonel West's Misguided Children.*"

Stardate 10909.18

At the Third Brigade Muster, the unit was the Legion of Valor recipient for 2008. Additionally, 2LT Clark volunteered to write the Third Brigade's Newsletter, the *Cry Havoc!* (thereby joining the Third Brigade Staff.) He continued to hold this post until 11107.15, when he became Third Brigade S-1 (Personnel and Administration) instead.

Stardate 11104.16

Ship's Elections were held. BGN West stepped down as Ship's Captain, LTC Schugart stepped down as First Officer. Both also stopped participating in STARFLEET, the ship, and the 333rd MSG. Major Tank Clark was elected as ship's Captain, and appointed Commodore Liz Goulet as First Officer. Major Mike Tolleson was appointed as Second Officer of the *Regulator*, as Officer-In-Charge of the 333rd Marine Strike Group, and as Team Leader of the 33rd Rangers. Brevet-Colonel Tank Clark becomes DOIC of the 333rd MSG and the ATL of the 33rd Rangers.

Stardate 11106 (?)

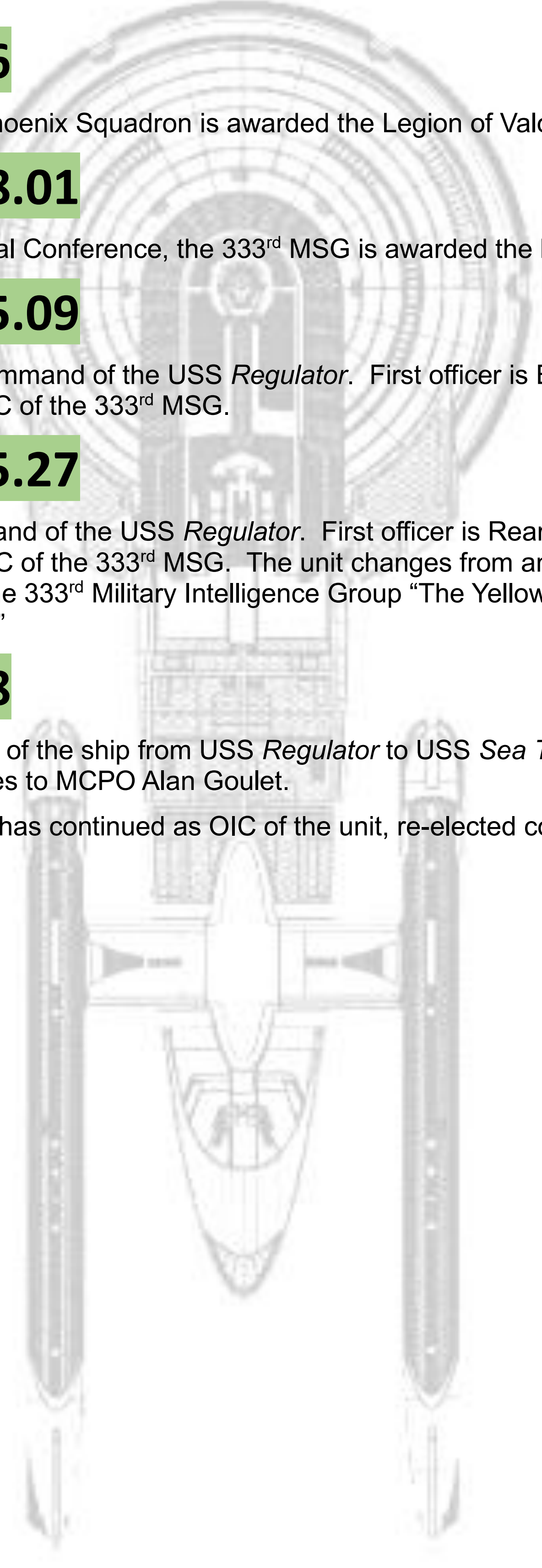
Members of the 333rd MSG decide to change from a Mecha unit to an Aerospace unit (as more of the members at this time are Aerospace than any other branch). The unit adopted its new nickname of "Phoenix Squadron," (suggested by LTC Tolleson) and chose "Numquam Cede, Numquam Succembe" ("Never Give Up, Never Surrender") – as suggested by Lieutenant Commander Cynthia Crouch.

Stardate 11107 (?)

At Third Brigade Muster, the 333rd MSG was the Legion of Valor recipient for the Third Brigade. Later in 2011, the unit received its first Legion of Honor award as well.

Stardate 11204 ?

LTC Colonel Tolleson transfers to USS *Navras*. Colonel Tank Clark becomes OIC of the 333rd MSG as well as TL of the 33rd Rangers. Lieutenant Commander Tracy Clark is appointed DOIC of the 333rd.



Stardate 11506

At Third Brigade Muster, Phoenix Squadron is awarded the Legion of Valor.

Stardate 11508.01

At STARFLEET International Conference, the 333rd MSG is awarded the Legion of Honor.

Stardate 11505.09

Michael Cross assumes command of the USS *Regulator*. First officer is Brigadier Tank Clark, and BDR Clark remains OIC of the 333rd MSG.

Stardate 11705.27

Tank Clark resumes command of the USS *Regulator*. First officer is Rear Admiral Liz Goulet, and BGN Clark remains OIC of the 333rd MSG. The unit changes from an Aerospace squadron to a Support Branch unit, the 333rd Military Intelligence Group “The Yellowjackets.” The new slogan is “We Know Better.”

Stardate 11708

Chapter changes the name of the ship from USS *Regulator* to USS *Sea Tiger.* The Deputy OIC of the Yellowjackets changes to MCPO Alan Goulet.

Since this time, Tank Clark has continued as OIC of the unit, re-elected continuously.

3.0 Traditions of the 333rd

3.1 Nickname

The nickname of the 333rd Marine Strike Group is the “Yellowjackets.” We also refer to the group as a Military Intelligence Group, in accordance with Support Branch procedures.

3.2 Slogan

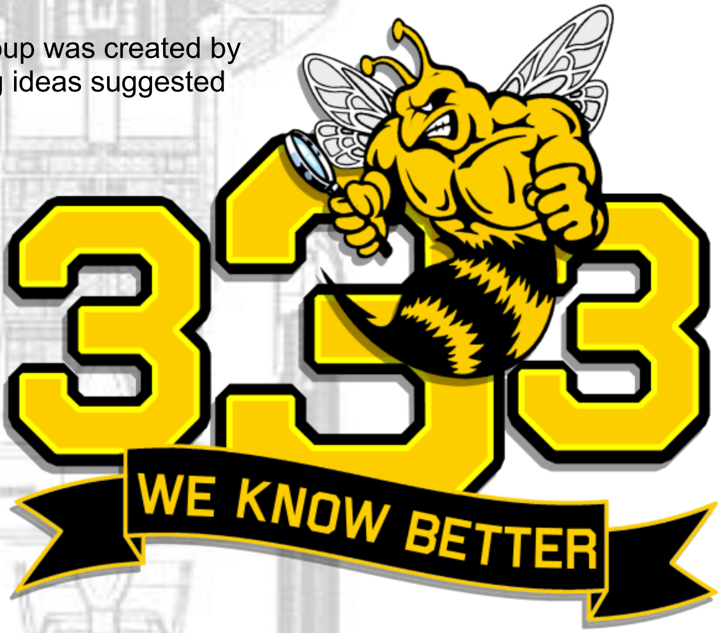
The slogan of the 333rd Marine Strike Group is “We Know Better”.

3.3 Motto

The motto of the 333rd MSG is “Ad discendum et ad certiorem” (To Learn and To Notify) This represents what an Intelligence unit does: it learns information, and discriminates it.

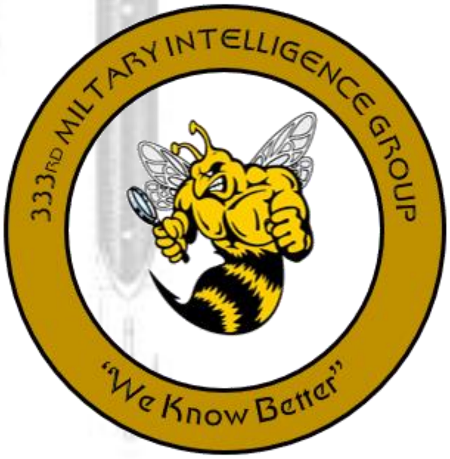
3.4 Logo

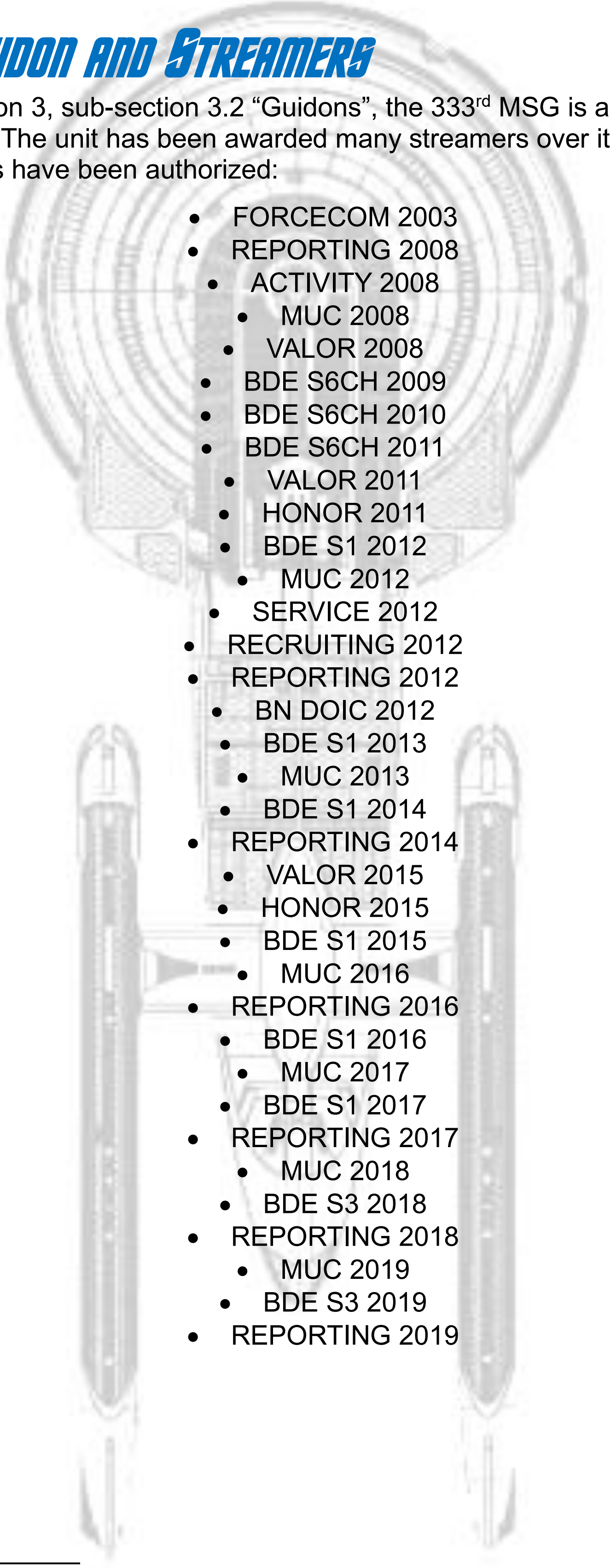
The logo for the Military Intelligence Group was created by Col Brian Allen (COFORCECOM), using ideas suggested by members of the 333rd.



3.5 MILINTGRU Patch

The unit’s patch is a simplified version of the logo.





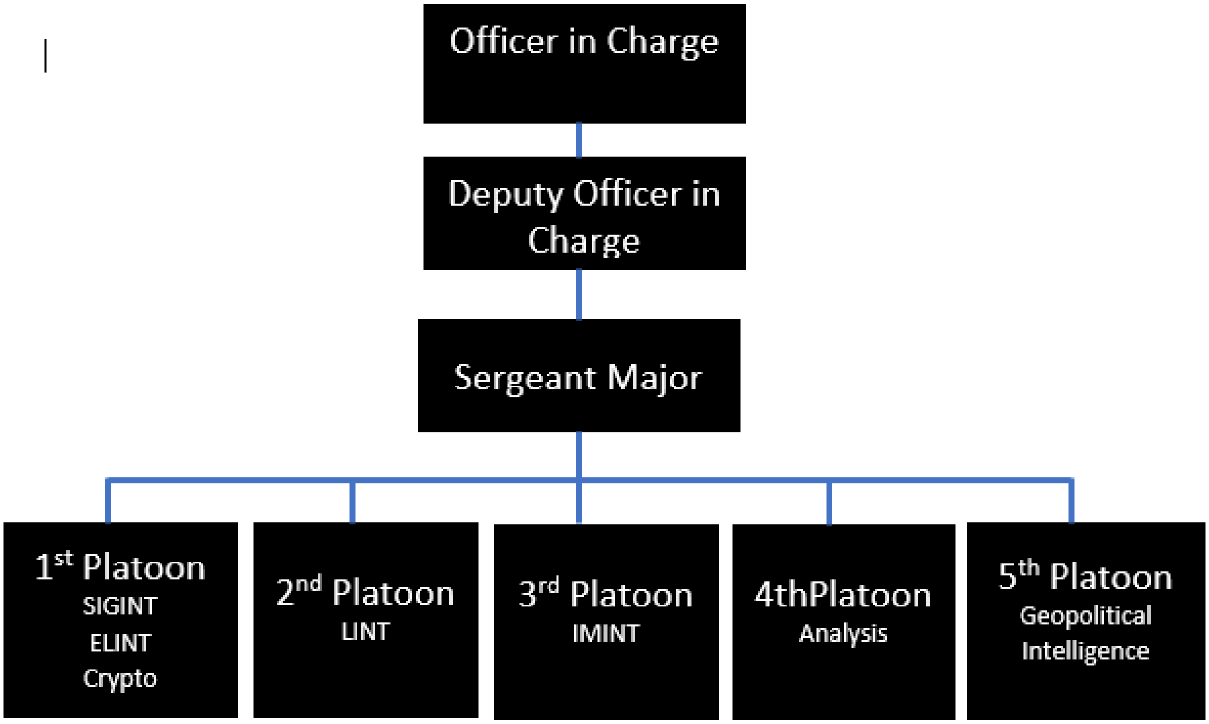
3.6 Unit's Guidon and Streamers

As per the MFM, Section 3, sub-section 3.2 “Guidons”, the 333rd MSG is authorized to carry or display a unit Guidon. The unit has been awarded many streamers over its existence[1]. To date, the following streamers have been authorized:

- FORCECOM 2003
- REPORTING 2008
- ACTIVITY 2008
- MUC 2008
- VALOR 2008
- BDE S6CH 2009
- BDE S6CH 2010
- BDE S6CH 2011
- VALOR 2011
- HONOR 2011
- BDE S1 2012
- MUC 2012
- SERVICE 2012
- RECRUITING 2012
- REPORTING 2012
- BN DOIC 2012
- BDE S1 2013
- MUC 2013
- BDE S1 2014
- REPORTING 2014
- VALOR 2015
- HONOR 2015
- BDE S1 2015
- MUC 2016
- REPORTING 2016
- BDE S1 2016
- MUC 2017
- BDE S1 2017
- REPORTING 2017
- MUC 2018
- BDE S3 2018
- REPORTING 2018
- MUC 2019
- BDE S3 2019
- REPORTING 2019

[1] See the current MFM for more details on streamers

4.0 Table of Organization



Officer in Charge

Deputy Officer in Charge

Sergeant Major

1st Platoon
SIGINT
ELINT
Crypto

2nd Platoon
LINT

3rd Platoon
IMINT

4thPlatoon
Analysis

5th Platoon
Geopolitical Intelligence

5.0 Uniforms

No uniforms are required by either the USS Sea Tiger or by the SFMC. However, any uniforms worn should be worn in accordance with the guidelines set forth by STARFLEET Marine Corps, this guidebook, and the *USS* Sea Tiger *Uniform Guidebook.*

5.1 SFMC Guidelines

Refer to the SFMC Uniform Policies and Guidelines, for details on STARFLEET Marine Corps authorized uniforms. Uniforms are not required, but in some situations they are highly encouraged.

5.2 333rd MSG Guidelines

All uniforms described in the SFMC Uniform Policies and Guidelines are authorized for wear by members of the 333rd MSG.

Some "off-the-rack" style uniforms are not immediately recognizable as Trek uniforms, specifically the Battle Dress Uniform (BDU), the Flight Suit, and the Vehicle Crew Garment. Exercise judgement when wearing these, especially at a public venue. In recent years, people wearing all-black BDUs not dissimilar to those worn by the SFMC have behaved very badly. (For example, in the 2012 Aurora, Colorado movie cinema shooting, the gunman was wearing black BDUs, a gas mask, and body armor.) **Wearing SFMC uniforms that follow general Star Trek styles is more appropriate.**

A member of the 333rd MSG may wear a non-Marine uniform from a different division, as desired, when not performing duties as a Marine. However, if acting as a Marine, the use of SFMC specific uniforms are recommended. See the *USS Sea Tiger Uniform Guidebook* for a detailed overview of various uniforms.

Following a discussion with the MSG, the OIC has authorized a "local uniform" in the TOS style, in which an olive drab tunic – in the style of the SFMC charcoal grey TOS tunic -- is worn. The sleeve rank cuffs use an alternate, subdued color as well, replacing the gold with black.

5.2.1 Headgear

Each uniform described in the SFMC MFM has a listing for headgear. The black beret is wearable with most uniforms, but some uniforms also allow a black eight-point cover, a ball cap, or a "boonie." No Class A uniforms have authorized headgear.

Members of the 333rd are also permitted to wear a black garrison cap, with or without trim in the color of their Branch of Service (or with Black trim). (A previous Third Brigade OIC has authorized them, at least with our unit, and none of his successors have rescinded this permission.)

See the SFMC Uniform Policies and Guidelines and the *USS Sea Tiger Uniform Guidebook* for more information on covers.

Black berets may be purchased from Glendale (Parade Store), at http://www.paradestore.com/index.php/our-products/berets-helmets/armed-forces-berets.html

6.0 Stuff and Things

6.1 What does the 333rd Marine Strike Group (“‘Yellowjackets’”) do?

First and foremost, members of the 333rd Military Intelligence Group are members of the USS *Sea Tiger*, the Fort Worth (Texas) Chapter of STARFLEET, the International Star Trek Fan Association, Inc. As such, we may participate in any and all activities of the USS *Sea Tiger* and the ship's Division which we have chosen, as well as any Zone, Regional, or International event of Zone 1, Region 3, or STARFLEET.

Secondly, members of the 333rd MSG are strongly encouraged to take courses from the STARFLEET Marine Academy, especially in the schools of Leadership, Professional Development, and the Support Branch, especially SU-100, SU-201, and SU-250. Courses from the Institute of Intelligence and Espionage at STARFLEET Academy are also encouraged.

Thirdly, the Marines, functioning in many ways in a similar manner to a Division on the USS *Sea Tiger* (although we are not technically a Division, per se), are the organizers of any ship's activities that the Group deems appropriate. Tabletop wargames of both tactical and strategic natures, like “Axis and Allies” and “Sixth Fleet”, are a good example. Trivia games are another.

Finally, the Yellowjackets may be given other real-world tasks, as deemed necessary and appropriate, by the Command Staff of the USS *Sea Tiger*.

6.2 Mission

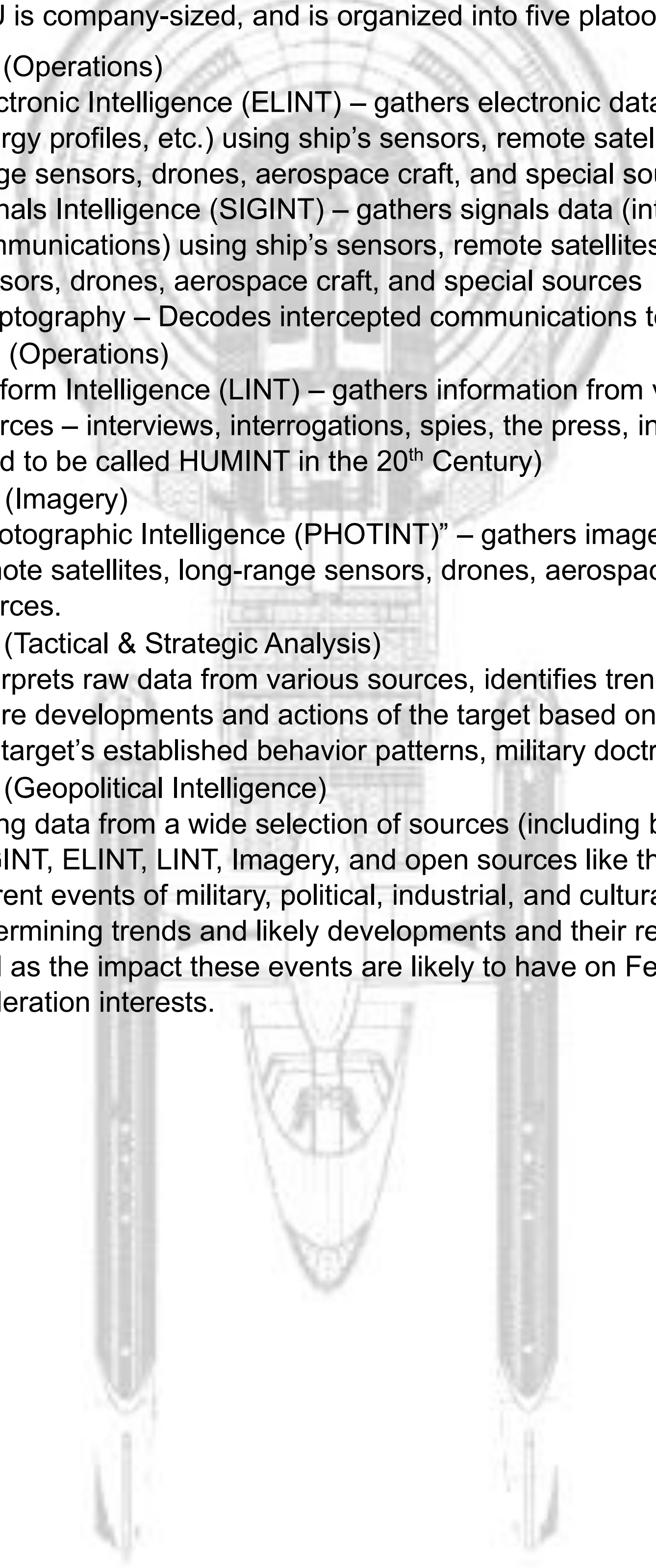
The mission of the 333rd Military Intelligence Group is to provide Military Intelligence and Intelligence support to all Marine units of the Third Brigade.

6.2 Organization of the 333rd Military Intelligence Group

See also section 7 for a more detailed examination of the tasks in which each platoon engages.

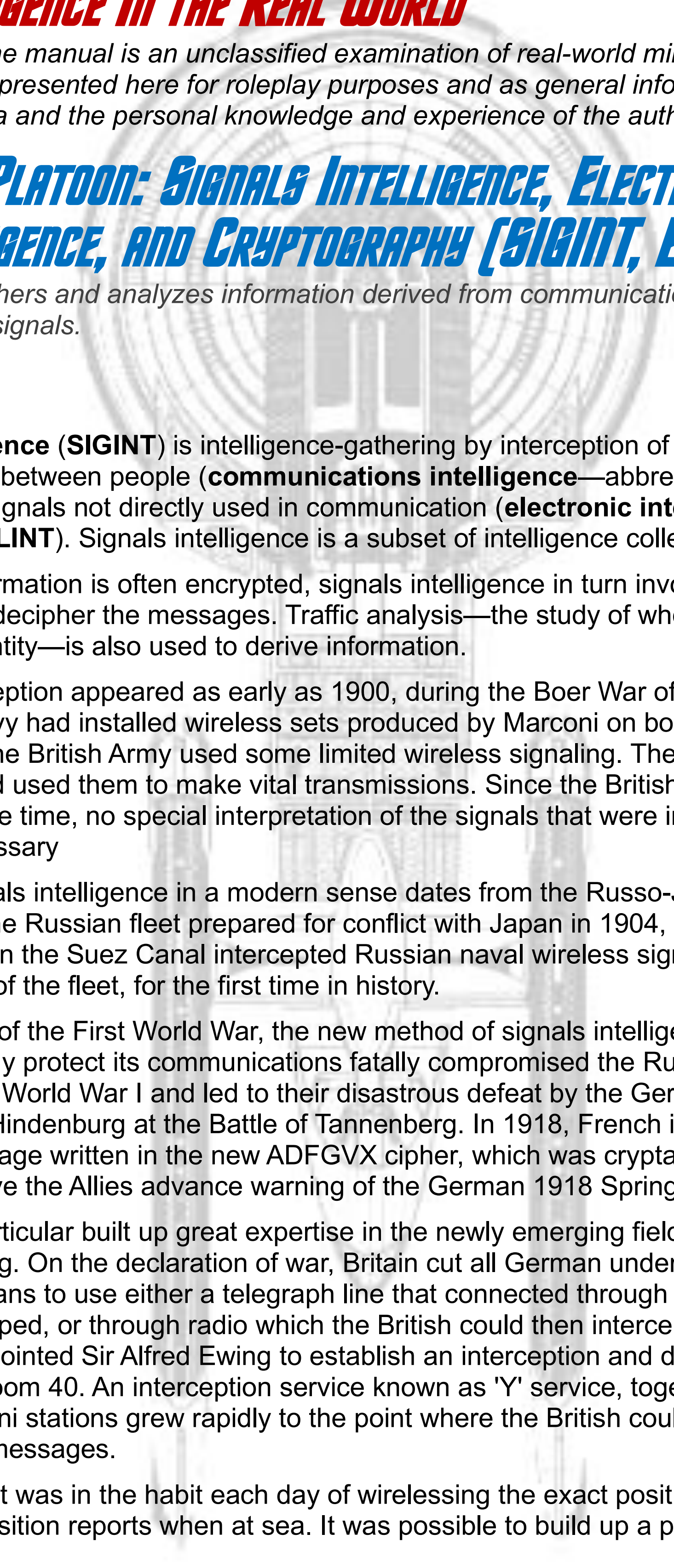
The 333rd MILINTGRU is company-sized, and is organized into five platoons:

- 1st Platoon (Operations)
  - Electronic Intelligence (ELINT) – gathers electronic data (scanner emissions, energy profiles, etc.) using ship's sensors, remote satellites, probes, long-range sensors, drones, aerospace craft, and special sources
  - Signals Intelligence (SIGINT) – gathers signals data (intercepted communications) using ship's sensors, remote satellites, probes, long-range sensors, drones, aerospace craft, and special sources
  - Cryptography – Decodes intercepted communications to permit analysis.
- 2nd Platoon (Operations)
  - Lifeform Intelligence (LINT) – gathers information from various life-form sources – interviews, interrogations, spies, the press, informants, etc. (what used to be called HUMINT in the 20th Century)
- 3rd Platoon (Imagery)
  - "Photographic Intelligence (PHOTINT)" – gathers images from ship's sensors, remote satellites, long-range sensors, drones, aerospace craft, and special sources.
- 4th Platoon (Tactical & Strategic Analysis)
  - Interprets raw data from various sources, identifies trends, deduces probable future developments and actions of the target based on historical tendencies, the target's established behavior patterns, military doctrine, and culture.
- 5th Platoon (Geopolitical Intelligence)
  - Using data from a wide selection of sources (including but not limited to SIGINT, ELINT, LINT, Imagery, and open sources like the press), analyzes current events of military, political, industrial, and cultural natures, determining trends and likely developments and their relative importance, as well as the impact these events are likely to have on Federation forces and Federation interests.



7.0 Intelligence In the Real World

This section of the manual is an unclassified examination of real-world military/naval intelligence. It is presented here for roleplay purposes and as general information. Sources include Wikipedia and the personal knowledge and experience of the author (Tank Clark).



7.1 First Platoon: Signals Intelligence, Electronics Intelligence, and Cryptography (SIGINT, ELINT, Crypto)

First Platoon gathers and analyzes information derived from communications, electronic, and instrumentation signals.

SIGINT

Signals intelligence (**SIGINT**) is intelligence-gathering by interception of signals, whether communications between people (**communications intelligence**—abbreviated to **COMINT**) or from electronic signals not directly used in communication (**electronic intelligence**—abbreviated to **ELINT**). Signals intelligence is a subset of intelligence collection management.

As sensitive information is often encrypted, signals intelligence in turn involves the use of cryptanalysis to decipher the messages. Traffic analysis—the study of who is signaling whom and in what quantity—is also used to derive information.

Electronic interception appeared as early as 1900, during the Boer War of 1899-1902. The British Royal Navy had installed wireless sets produced by Marconi on board their ships in the late 1890s and the British Army used some limited wireless signaling. The Boers captured some wireless sets and used them to make vital transmissions. Since the British were the only people transmitting at the time, no special interpretation of the signals that were intercepted by the British was necessary

The birth of signals intelligence in a modern sense dates from the Russo-Japanese War of 1904-1905. As the Russian fleet prepared for conflict with Japan in 1904, the British ship HMS *Diana* stationed in the Suez Canal intercepted Russian naval wireless signals being sent out for the mobilization of the fleet, for the first time in history.

Over the course of the First World War, the new method of signals intelligence reached maturity. Failure to properly protect its communications fatally compromised the Russian Army in its advance early in World War I and led to their disastrous defeat by the Germans under Ludendorff and Hindenburg at the Battle of Tannenberg. In 1918, French intercept personnel captured a message written in the new ADFGVX cipher, which was cryptanalyzed by Georges Painvin. This gave the Allies advance warning of the German 1918 Spring offensive.

The British in particular built up great expertise in the newly emerging field of signals intelligence and codebreaking. On the declaration of war, Britain cut all German undersea cables. This forced the Germans to use either a telegraph line that connected through the British network and could be tapped, or through radio which the British could then intercept. Rear-Admiral Henry Oliver appointed Sir Alfred Ewing to establish an interception and decryption service at the Admiralty; Room 40. An interception service known as 'Y' service, together with the post office and Marconi stations grew rapidly to the point where the British could intercept almost all official German messages.

The German fleet was in the habit each day of wirelessing the exact position of each ship and giving regular position reports when at sea. It was possible to build up a precise picture of the normal operation of the High Seas Fleet, to infer from the routes they chose where defensive minefields had been placed and where it was safe for ships to operate. Whenever a change to the normal pattern was seen, it immediately signaled that some operation was about to take place and a warning could be given. Detailed information about submarine movements was also available.

The use of radio receiving equipment to pinpoint the location of the transmitter was also developed during the war. Captain H.J. Round working for Marconi, began carrying out experiments with direction finding radio equipment for the army in France in 1915. By May 1915, the Admiralty was able to track German submarines crossing the North Sea. Some of these stations also acted as 'Y' stations to collect German messages, but a new section was created within Room 40 to plot the positions of ships from the directional reports.

Room 40 played an important role in several naval engagements during the war, notably in detecting major German sorties into the North Sea. The battle of Dogger Bank was won in no small part due to the intercepts that allowed the Navy to position its ships in the right place. It played a vital role in subsequent naval clashes, including at the Battle of Jutland as the British fleet was sent out to intercept them. The direction-finding capability allowed for the tracking and location of German ships, submarines and Zeppelins. The system was so successful, that by the end of the war over 80 million words, comprising the totality of German wireless transmission over the course of the war had been intercepted by the operators of the Y-stations and decrypted.[1] However its most astonishing success was in decrypting the Zimmermann Telegram, a telegram from the German Foreign Office sent via Washington to its ambassador Heinrich von Eckardt in Mexico.

With the importance of interception and decryption firmly established by the wartime experience, countries established permanent agencies dedicated to this task in the interwar period. In 1919, the British Cabinet's Secret Service Committee, chaired by Lord Curzon, recommended that a peace-time codebreaking agency should be created. The Government Code and Cypher School (GC&CS) was the first peace-time codebreaking agency, with a public function "to advise as to the security of codes and cyphers used by all Government departments and to assist in their provision", but also with a secret directive to "study the methods of cypher communications used by foreign powers". GC&CS officially formed on 1 November 1919, and produced its first decrypt on 19 October. By 1940, GC&CS was working on the diplomatic codes and ciphers of 26 countries, tackling over 150 diplomatic cryptosystems.

The US Cipher Bureau was established in 1919 and achieved some success at the Washington Naval Conference in 1921, through cryptanalysis by Herbert Yardley. Secretary of War Henry L. Stimson closed the US Cipher Bureau in 1929 with the words "Gentlemen do not read each other's mail."

The use of SIGINT had even greater implications during World War II. The combined effort of intercepts and cryptanalysis for the whole of the British forces in World War II came under the code name "Ultra" managed from Government Code and Cypher School at Bletchley Park. Properly used, the German Enigma and Lorenz ciphers should have been virtually unbreakable, but flaws in German cryptographic procedures, and poor discipline among the personnel carrying them out, created vulnerabilities which made Bletchley's attacks feasible.

Bletchley's work was essential to defeating the U-boats in the Battle of the Atlantic, and to the British naval victories in the Battle of Cape Matapan and the Battle of North Cape. In 1941, Ultra exerted a powerful effect on the North African desert campaign against German forces under General Erwin Rommel. General Sir Claude Auchinleck wrote that were it not for Ultra, "Rommel would have certainly got through to Cairo". "Ultra" decrypts featured prominently in the story of Operation SALAM, László Almásy's mission across the desert behind Allied lines in 1942. Prior to the Normandy landings on D-Day in June 1944, the Allies knew the locations of all but two of Germany's fifty-eight Western-front divisions.

Winston Churchill was reported to have told King George VI: "It is thanks to the secret weapon of General Menzies, put into use on all the fronts, that we won the war!" Supreme Allied Commander, Dwight D. Eisenhower, at the end of the war, described Ultra as having been "decisive" to Allied victory. Official historian of British Intelligence in World War II Sir Harry Hinsley, argued that Ultra shortened the war "by not less than two years and probably by four years"; and that, in the absence of Ultra, it is uncertain how the war would have ended.

Definitions:

The United States Department of Defense has defined the term "signals intelligence" as:

- A category of intelligence comprising either individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence, however transmitted.
- Intelligence derived from communications, electronic, and foreign instrumentation signals.

Being a broad field, SIGINT has many sub-disciplines. The two main ones are communications intelligence (COMINT) and electronic intelligence (ELINT).

Targeting:

A collection system has to know to look for a particular signal. "System", in this context, has several nuances. Targeting is an output of the process of developing *collection requirements*:

- An intelligence need considered in the allocation of intelligence resources. Within the Department of Defense, these collection requirements fulfill the essential elements of information and other intelligence needs of a commander, or an agency.
- An established intelligence need, validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer."

Need for multiple, coordinated receivers:

First, atmospheric conditions, sunspots, the target's transmission schedule and antenna characteristics, and other factors create uncertainty that a given signal intercept sensor will be able to "hear" the signal of interest, even with a geographically fixed target and an opponent making no attempt to evade interception. Basic countermeasures against interception include frequent changing of radio frequency, polarization, and other transmission characteristics. An intercept aircraft could not get off the ground if it had to carry antennas and receivers for every possible frequency and signal type to deal with such countermeasures.

Second, locating the transmitter's position is usually part of SIGINT. Triangulation and more sophisticated radio location techniques, such as time of arrival methods, require multiple receiving points at different locations. These receivers send location-relevant information to a central point, or perhaps to a distributed system in which all participate, such that the information can be correlated, and a location computed.

Intercept management:

Modern SIGINT systems, therefore, have substantial communications among intercept platforms. Even if some platforms are clandestine, there is still a broadcast of information telling them where and how to look for signals. A United States targeting system under development in the late 1990s, PSTS, constantly sends out information that helps the interceptors properly aim their antennas and tune their receivers. Larger intercept aircraft, such as the EP-3 or RC-135, have the on-board capability to do some target analysis and planning, but others, such as the RC-12 GUARDRAIL, are completely under ground direction. GUARDRAIL aircraft are fairly small, and usually work in units of three to cover a tactical SIGINT requirement, where the larger aircraft tend to be assigned strategic/national missions.

Before the detailed process of targeting begins, someone has to decide there is a value in collecting information about something. While it would be possible to direct signals intelligence collection at a major sports event, the systems would capture a great deal of noise, news signals, and perhaps announcements in the stadium. If, however, an anti-terrorist organization believed that a small group would be trying to coordinate their efforts, using short-range unlicensed radios, at the event, SIGINT targeting of radios of that type would be reasonable. Targeting would not know where in the stadium the radios might be located, or the exact frequency they are using; those are the functions of subsequent steps such as signal detection and direction finding.

Once the decision to target is made, the various interception points need to cooperate, since resources are limited. Knowing what interception equipment to use becomes easier when a target country buys its radars and radios from known manufacturers or is given them as military aid. National intelligence services keep libraries of devices manufactured by their own country and others, and then use a variety of techniques to learn what equipment is acquired by a given country.

Knowledge of physics and electronic engineering further narrows the problem of what types of equipment might be in use. An intelligence aircraft flying well outside the borders of another country will listen for long-range search radars, not short-range fire control radars that would be used by a mobile air defense. Soldiers scouting the front lines of another army know that the other side will be using radios that must be portable and not have huge antennas.

SIGNAL DETECTION:

Even if a signal is human communications (e.g., a radio), the intelligence collection specialists have to know it exists. If the targeting function described above learns that a country has a radar that operates in a certain frequency range, the first step is to use a sensitive receiver, with one or more antennas that listen in every direction, to find an area where such a radar is operating. Once the radar is known to be in the area, the next step is to find its location.

If operators know the probable frequencies of transmissions of interest, they may use a set of receivers, preset to the frequencies of interest. These are the frequency (horizontal axis) versus power (vertical axis) produced at the transmitter, before any filtering of signals that do not add to the information being transmitted. Received energy on a particular frequency may start a recorder and alert a human to listen to the signals if they are intelligible (i.e., COMINT). If the frequency is not known, the operators may look for power on primary or sideband frequencies using a spectrum analyzer. Information from the spectrum analyzer is then used to tune receivers to signals of interest. Real-world transmitters and receivers usually are directional.

Spread-spectrum communications is an electronic counter-countermeasures (ECCM) technique to defeat looking for particular frequencies. Spectrum analysis can be used in a different ECCM way to identify frequencies not being jammed or not in use.

DIRECTION FINDING:

The earliest, and still common, means of direction finding is to use directional antennas as goniometers, so that a line can be drawn from the receiver through the position of the signal of interest. Knowing the compass bearing, from a single point, to the transmitter does not locate it. Where the bearings from multiple points, using goniometry, are plotted on a map, the transmitter will be located at the point where the bearings intersect. This is the simplest case; a target may try to confuse listeners by having multiple transmitters, giving the same signal from different locations, switching on and off in a pattern known to their user but apparently random to the listener.

Individual directional antennas have to be manually or automatically turned to find the signal direction, which may be too slow when the signal is of short duration. One alternative is the Wullenweber array technique. In this method, several concentric rings of antenna elements simultaneously receive the signal, so that the best bearing will ideally be clearly on a single antenna or a small set. Wullenweber arrays for high-frequency signals are enormous, referred to as "elephant cages" by their users.

An alternative to tunable directional antennas, or large omnidirectional arrays such as the Wullenweber, is to measure the time of arrival of the signal at multiple points, using GPS or a similar method to have precise time synchronization. Receivers can be on ground stations, ships, aircraft, or satellites, giving great flexibility.

Modern anti-radiation missiles can home in on and attack transmitters; military antennas are rarely a safe distance from the user of the transmitter.

Traffic analysis

When locations are known, usage patterns may emerge, from which inferences may be drawn. Traffic analysis is the discipline of drawing patterns from information flow among a set of senders and receivers, whether those senders and receivers are designated by location determined through direction finding, by addressee and sender identifications in the message, or even MASINT techniques for "fingerprinting" transmitters or operators. Message content, other than the sender and receiver, is not necessary to do traffic analysis, although more information can be helpful.

For example, if a certain type of radio is known to be used only by tank units, even if the position is not precisely determined by direction finding, it may be assumed that a tank unit is in the general area of the signal. The owner of the transmitter can assume someone is listening, so might set up tank radios in an area where he wants the other side to believe he has actual tanks. As part of Operation Quicksilver, part of the deception plan for the invasion of Europe at the Battle of Normandy, radio transmissions simulated the headquarters and subordinate units of the fictitious First United States Army Group (FUSAG), commanded by George S. Patton, to make the German defense think that the main invasion was to come at another location. In like manner, fake radio transmissions from Japanese aircraft carriers, before the Battle of Pearl Harbor, were made from Japanese local waters, while the attacking ships moved under strict radio silence.

Traffic analysis need not focus on human communications. For example, if the sequence of a radar signal, followed by an exchange of targeting data and a confirmation, followed by observation of artillery fire, this may identify an automated counterbattery system. A radio signal that triggers navigational beacons could be a landing aid system for an airstrip or helicopter pad that is intended to be low-profile.

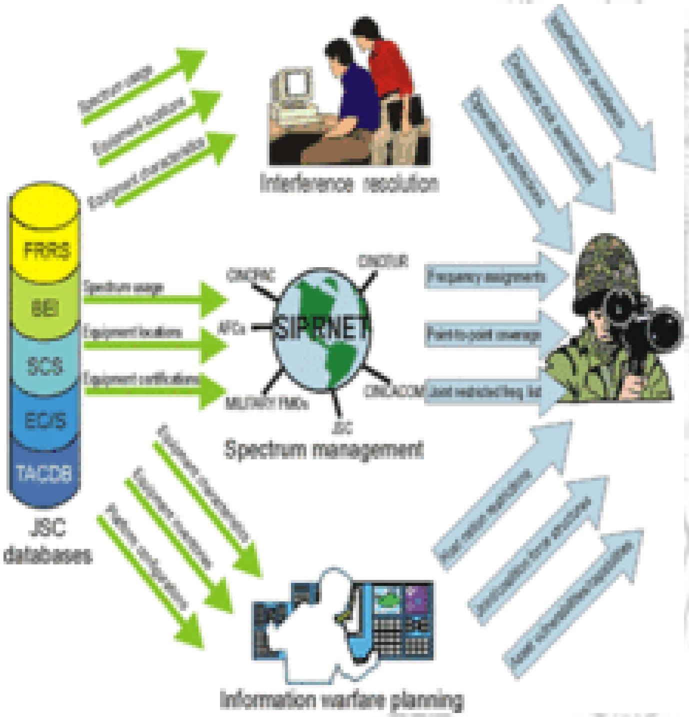
Patterns do emerge. Knowing a radio signal, with certain characteristics, originating from a fixed headquarters may be strongly suggestive that a particular unit will soon move out of its regular base. The contents of the message need not be known to infer the movement.

There is an art as well as science of traffic analysis. Expert analysts develop a sense for what is real and what is deceptive. Harry Kidder, for example, was one of the star cryptanalysts of World War II, a star hidden behind the secret curtain of SIGINT.

ELECTRONIC ORDER-OF-BATTLE:

Generating an **electronic order of battle** (EOB) requires identifying SIGINT emitters in an area of interest, determining their geographic location or range of mobility, characterizing their signals, and, where possible, determining their role in the broader organizational order of battle. EOB covers both COMINT and ELINT. The Defense Intelligence Agency maintains an EOB by location. The Joint Spectrum Center (JSC) of the Defense Information Systems Agency supplements this location database with five more technical databases:

- FRRS: Frequency Resource Record System
- BEI: Background Environment Information
- SCS: Spectrum Certification System
- EC/S: Equipment Characteristics/Space
- TACDB: platform lists, sorted by nomenclature, which contain links to the C-E equipment complement of each platform, with links to the parametric data for each piece of equipment, military unit lists and their subordinate units with equipment used by each unit.



For example, several voice transmitters might be identified as the command net (i.e., top commander and direct reports) in a tank battalion or tank-heavy task force. Another set of transmitters might identify the logistic net for that same unit. An inventory of ELINT sources might identify the medium- and long-range counter-artillery radars in a given area.

Signals intelligence units will identify changes in the EOB, which might indicate enemy unit movement, changes in command relationships, and increases or decreases in capability.

Using the COMINT gathering method enables the intelligence officer to produce an electronic order of battle by traffic analysis and content analysis among several enemy units. For example, if the following messages were intercepted:

- U1 to U2, requesting permission to proceed to checkpoint X.
- U2 to U1, approved. please report at arrival.
- (20 minutes later) U1 to U2, all vehicles have arrived to checkpoint X.

This sequence shows that there are two units in the battlefield, unit 1 is mobile, while unit 2 is in a higher hierarchical level, perhaps a command post. One can also understand that unit 1 moved from one point to another which are 20 minutes apart with a vehicle. If these are regular reports over a period of time, they might reveal a patrol pattern. Direction-finding and radiofrequency MASINT could help confirm that the traffic is not deception.

The EOB buildup process is divided as following:

- Signal separation
- Measurements optimization
- Data Fusion
- Networks build-up

Separation of the intercepted spectrum and the signals intercepted from each sensor must take place in an extremely small period of time, in order to separate the deferent signals to different transmitters in the battlefield. The complexity of the separation process depends on the complexity of the transmission methods (e.g., hopping or time division multiple access (TDMA)).

By gathering and clustering data from each sensor, the measurements of the direction of signals can be optimized and get much more accurate than the basic measurements of a standard direction finding sensor. By calculating larger samples of the sensor's output data in near real-time, together with historical information of signals, better results are achieved.

Data fusion correlates data samples from different frequencies from the same sensor, "same" being confirmed by direction finding or radiofrequency MASINT. If an emitter is mobile, direction finding, other than discovering a repetitive pattern of movement, is of limited value in determining if a sensor is unique. MASINT then becomes more informative, as individual transmitters and antennas may have unique side lobes, unintentional radiation, pulse timing, etc.

Network build-up, or analysis of emitters (communication transmitters) in a target region over a sufficient period of time, enables creation of the communications flows of a battlefield.

COMINT

COMINT (Communications Intelligence) is a sub-category of signals intelligence that engages in dealing with messages or voice information derived from the interception of foreign communications. It should be noted that COMINT is commonly referred to as SIGINT, which can cause confusion when talking about the broader intelligence disciplines. The US Joint Chiefs of Staff defines it as "Technical information and intelligence derived from foreign communications by other than the intended recipients".

COMINT, which is defined to be communications among people, will reveal some or all of the following:

1. Who is transmitting
2. Where they are located, and, if the transmitter is moving, the report may give a plot of the signal against location
3. If known, the organizational function of the transmitter
4. The time and duration of transmission, and the schedule if it is a periodic transmission
5. The frequencies and other technical characteristics of their transmission
6. If the transmission is encrypted or not, and if it can be decrypted. If it is possible to intercept either an originally transmitted cleartext or obtain it through cryptanalysis, the language of the communication and a translation (when needed).
7. The addresses, if the signal is not a general broadcast and if addresses are retrievable from the message. These stations may also be COMINT (e.g., a confirmation of the message or a response message), ELINT (e.g., a navigation beacon being activated) or both. Rather than, or in addition to, an address or other identifier, there may be information on the location and signal characteristics of the responder.

VOICE INTERCEPTION

A basic COMINT technique is to listen for voice communications, usually over radio but possibly "leaking" from telephones or from wiretaps. If the voice communications are encrypted, traffic analysis may still give information.

In the Second World War, for security the United States used Native American volunteer communicators known as code talkers, who used languages such as Navajo, Comanche and Choctaw, which would be understood by few people, even in the U.S. Even within these uncommon languages, the code talkers used specialized codes, so a "butterfly" might be a specific Japanese aircraft. British forces made limited use of Welsh speakers for the same reason.

While modern electronic encryption does away with the need for armies to use obscure languages, it is likely that some groups might use rare dialects that few outside their ethnic group would understand.

TEXT INTERCEPTION

Morse code interception was once very important, but Morse code telegraphy is now obsolete in the western world, although possibly used by special operations forces. Such forces, however, now have portable cryptographic equipment. Morse code is still used by military forces of former Soviet Union countries.

Specialists scan radio frequencies for character sequences (e.g., electronic mail) and fax.

SIGNALING CHANNEL INTERCEPTION

A given digital communications link can carry thousands or millions of voice communications, especially in developed countries. Without addressing the legality of such actions, the problem of identifying which channel contains which conversation becomes much simpler when the first thing intercepted is the *signaling channel* that carries information to set up telephone calls. In civilian and many military use, this channel will carry messages in Signaling System 7 protocols.

Retrospective analysis of telephone calls can be made from Call detail record (CDR) used for billing the calls.

MONITORING FRIENDLY COMMUNICATIONS

More a part of communications security than true intelligence collection, SIGINT units still may have the responsibility of monitoring one's own communications or other electronic emissions, to avoid providing intelligence to the enemy. For example, a security monitor may hear an individual transmitting inappropriate information over an unencrypted radio network, or simply one that is not authorized for the type of information being given. If immediately calling attention to the violation would not create an even greater security risk, the monitor will call out one of the BEADWINDOW codes used by Australia, Canada, New Zealand, the United Kingdom, the United States, and other nations working under their procedures. Standard BEADWINDOW codes (e.g., "BEADWINDOW 2") include:

1. **Position:** (e.g., disclosing, in an insecure or inappropriate way, "Friendly or enemy position, movement or intended movement, position, course, speed, altitude or destination or any air, sea or ground element, unit or force."
2. **Capabilities:** "Friendly or enemy capabilities or limitations. Force compositions or significant casualties to special equipment, weapons systems, sensors, units or personnel. Percentages of fuel or ammunition remaining."
3. **Operations:** "Friendly or enemy operation – intentions progress, or results. Operational or logistic intentions; mission participants flying programmes; mission situation reports; results of friendly or enemy operations; assault objectives."
4. **Electronic warfare (EW):** "Friendly or enemy electronic warfare (EW) or emanations control (EMCON) intentions, progress, or results. Intention to employ electronic countermeasures (ECM); results of friendly or enemy ECM; ECM objectives; results of friendly or enemy electronic counter-countermeasures (ECCM); results of electronic support measures/tactical SIGINT (ESM); present or intended EMCON policy; equipment affected by EMCON policy."

5. **Friendly or enemy key personnel:** "Movement or identity of friendly or enemy officers, visitors, commanders; movement of key maintenance personnel indicating equipment limitations."
6. **Communications security (COMSEC):** "Friendly or enemy COMSEC breaches. Linkage of codes or codewords with plain language; compromise of changing frequencies or linkage with line number/circuit designators; linkage of changing call signs with previous call signs or units; compromise of encrypted/classified call signs; incorrect authentication procedure."
7. **Wrong circuit:** "Inappropriate transmission. Information requested, transmitted or about to be transmitted which should not be passed on the subject circuit because it either requires greater security protection or it is not appropriate to the purpose for which the circuit is provided."
8. Other codes as appropriate for the situation may be defined by the commander.

In WWII, for example, the Japanese Navy, by poor practice, identified a key person's movement over a low-security cryptosystem. This made possible Operation Vengeance, the interception and death of the Combined Fleet commander, Admiral Isoroku Yamamoto.

ELINT

Electronic signals intelligence (ELINT) refers to intelligence-gathering by use of electronic sensors. Its primary focus lies on non-communications signals intelligence. The Joint Chiefs of Staff define it as "Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources."

Signal identification is performed by analyzing the collected parameters of a specific signal, and either matching it to known criteria, or recording it as a possible new emitter. ELINT data are usually highly classified, and are protected as such.

The data gathered are typically pertinent to the electronics of an opponent's defense network, especially the electronic parts such as radars, surface-to-air missile systems, aircraft, etc. ELINT can be used to detect ships and aircraft by their radar and other electromagnetic radiation; commanders have to make choices between not using radar (EMCON), intermittently using it, or using it and expecting to avoid defenses. ELINT can be collected from ground stations near the opponent's territory, ships off their coast, aircraft near or in their airspace, or by satellite.

Complementary relationship to COMINT

Combining other sources of information and ELINT allows traffic analysis to be performed on electronic emissions which contain human encoded messages. The method of analysis differs from SIGINT in that any human encoded message which is in the electronic transmission is not analyzed during ELINT. What is of interest is the type of electronic transmission and its location. For example, during the Battle of the Atlantic in World War II, Ultra COMINT was not always available because Bletchley Park was not always able to read the U-boat Enigma traffic. But "Huff-Duff" (High Frequency Direction Finder -- HFDF) was still able to find where the U-boats were by analysis of radio transmissions and the positions through triangulation from the direction located by two or more Huff-Duff systems. The Admiralty was able to use this information to plot courses which took convoys away from high concentrations of U-boats.

Yet other ELINT disciplines include intercepting and analyzing enemy weapons control signals, or the Identification, friend or foe responses from transponders in aircraft used to distinguish enemy craft from friendly ones.

Role in air warfare

A very common area of ELINT is intercepting radars and learning their locations and operating procedures. Attacking forces may be able to avoid the coverage of certain radars, or, knowing their characteristics, electronic warfare units may jam radars or send them deceptive signals. Confusing a radar electronically is called a "soft kill", but military units will also send specialized missiles at radars, or bomb them, to get a "hard kill". Some modern air-to-air missiles also have radar homing guidance systems, particularly for use against large airborne radars.

Knowing where each surface-to-air missile and anti-aircraft artillery system is and its type means that air raids can be plotted to avoid the most heavily defended areas and to fly on a flight profile which will give the aircraft the best chance of evading ground fire and fighter patrols. It also allows for the jamming or spoofing of the enemy's defense network (see electronic warfare). Good electronic intelligence can be very important to stealth operations; stealth aircraft are not totally undetectable and need to know which areas to avoid. Similarly, conventional aircraft need to know where fixed or semi-mobile air defense systems are so that they can shut them down or fly around them.

ELINT and ESM

Electronic support measures (ESM) or **Electronic Surveillance Measures** are really ELINT techniques using various *Electronic Surveillance Systems*, but the term is used in the specific context of tactical warfare. ESM give the information needed for **electronic attack (EA)** such as jamming, or directional bearings (compass angle) to a target in *signals intercept* such as in the HUFF-DUFF Radio Direction Finding (RDF) systems so critically important during the WW-II Battle of the Atlantic. After WW-II, the RDF originally applied in only communications was broadened into systems to also take in ELINT from radar bandwidths and lower frequency communications systems, giving birth to a family of NATO ESM systems, such as the shipboard US AN/WLR-1—AN/WLR-6 systems and comparable airborne units. EA is also called **electronic counter-measures (ECM)**. ESM provides information needed for **electronic counter-counter measures (ECCM)**, such as understanding a spoofing or jamming mode so one can change one's radar characteristics to avoid them.

ELINT for meaconing

Meaconing is the combined intelligence and electronic warfare of learning the characteristics of enemy navigation aids, such as radio beacons, and retransmitting them with incorrect information.

Foreign instrumentation signals intelligence

FISINT (Foreign instrumentation signals intelligence) is a sub-category of SIGINT, monitoring primarily non-human communication. Foreign instrumentation signals include (but not limited to) telemetry (TELINT), tracking systems, and video data links. TELINT is an important part of national means of technical verification for arms control.

ELINT Versus MASINT

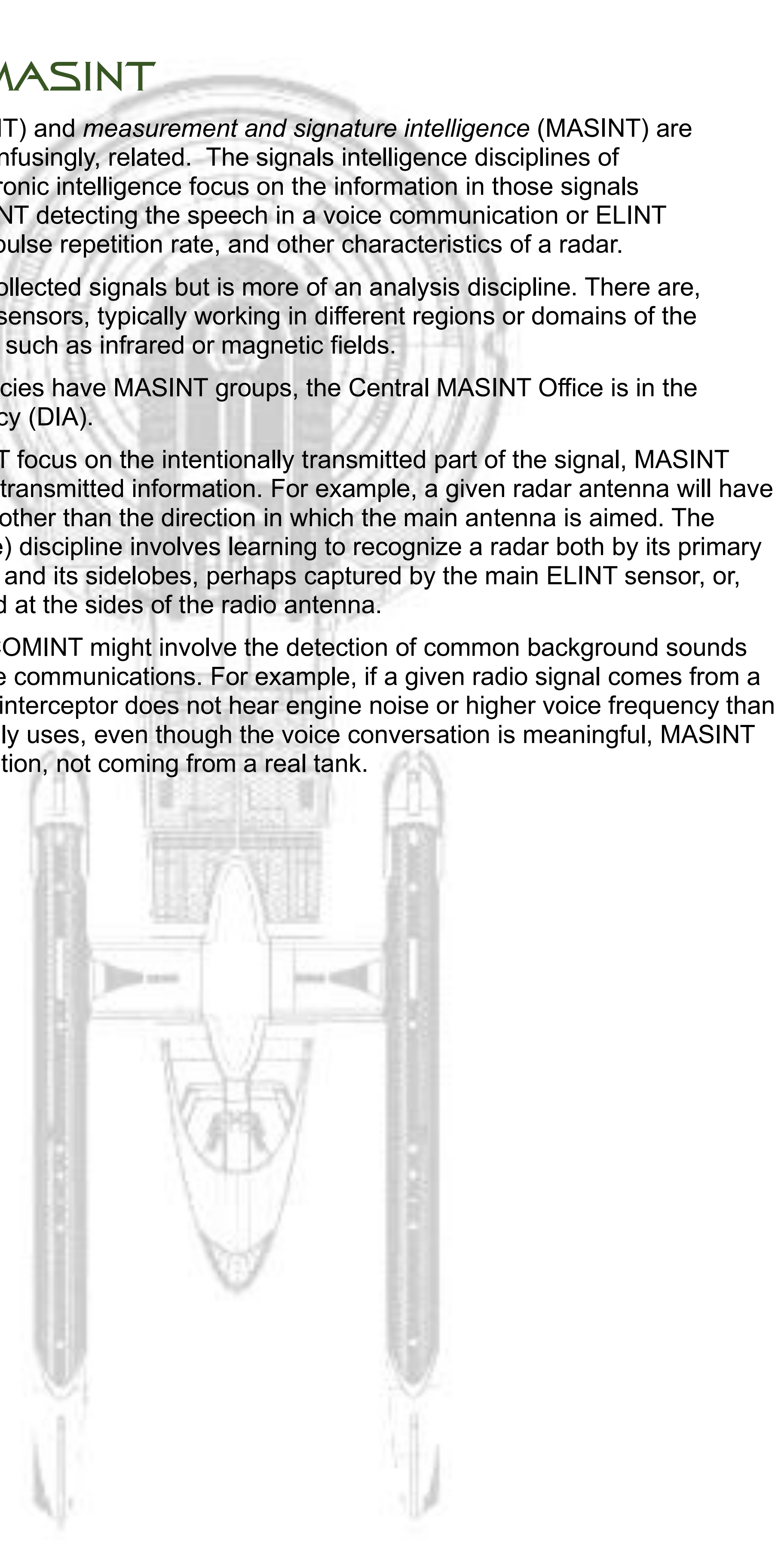
Signals intelligence (SIGINT) and *measurement and signature intelligence* (MASINT) are closely, and sometimes confusingly, related. The signals intelligence disciplines of communications and electronic intelligence focus on the information in those signals themselves, as with COMINT detecting the speech in a voice communication or ELINT measuring the frequency, pulse repetition rate, and other characteristics of a radar.

MASINT also works with collected signals but is more of an analysis discipline. There are, however, unique MASINT sensors, typically working in different regions or domains of the electromagnetic spectrum, such as infrared or magnetic fields.

While NSA and other agencies have MASINT groups, the Central MASINT Office is in the Defense Intelligence Agency (DIA).

Where COMINT and ELINT focus on the intentionally transmitted part of the signal, MASINT focuses on unintentionally transmitted information. For example, a given radar antenna will have sidelobes emanating from other than the direction in which the main antenna is aimed. The RADINT (radar intelligence) discipline involves learning to recognize a radar both by its primary signal, captured by ELINT, and its sidelobes, perhaps captured by the main ELINT sensor, or, more likely, a sensor aimed at the sides of the radio antenna.

MASINT associated with COMINT might involve the detection of common background sounds expected with human voice communications. For example, if a given radio signal comes from a radio used in a tank, if the interceptor does not hear engine noise or higher voice frequency than the voice modulation usually uses, even though the voice conversation is meaningful, MASINT might suggest it is a deception, not coming from a real tank.



7.2 Second Platoon: Lifeform Intelligence (LINT)

Second Platoon gathers and analyzes information from various life-form sources – interviews, interrogations, spies, the press, informants, etc. (what used to be called HUMINT in the 20th Century)

Lifeform intelligence (frequently abbreviated **LINT**) is intelligence gathered by means of interpersonal contact, as opposed to the more technical intelligence gathering disciplines such as signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signature intelligence (MASINT).

NATO defines HUMINT as "a category of intelligence derived from information collected and provided by human sources." Typical LINT activities consist of interrogations and conversations with persons having access to information.

The manner in which LINT operations are conducted is dictated by both official protocol and the nature of the source of the information. Within the context of the U.S. military, most HUMINT activity does not involve clandestine activities. Both counter intelligence and HUMINT do include clandestine HUMINT and clandestine HUMINT operational techniques.

HUMINT can provide several kinds of information. It can provide observations during travel or other events from travelers, refugees, escaped friendly POWs, etc. It can provide data on things about which the subject has specific knowledge, which can be another human subject, or, in the case of defectors and spies, sensitive information to which they had access. Finally, it can provide information on interpersonal relationships and networks of interest.

HUMINT is both a source of positive intelligence, but also of information of strong counterintelligence value. Interviews should balance any known information requirements of both intelligence collection guidance and of counterintelligence requirements.

Sources

Sources may be neutral, friendly, or hostile, and may or may not be witting [2]of their involvement in the collection of information.

Examples of LINT sources include, but are not limited to, the following:

- Advisors or foreign internal defense personnel working with host nation forces or populations
- Diplomatic reporting by accredited diplomats (like military attaches)
- Espionage clandestine reporting, access agents, couriers, cutouts
- Prisoners of War or Detainees
- Routine Patrolling (military police, patrols, etc)
- Special reconnaissance
- Traveler debriefing

Basic LINT Operations

Lifeform source screening is the logical start of collection of LINT. This involves selecting people who may be sources of meaningful intelligence, possibly positively identifying them, and conducting interviews of various types. Properly recording and cross-indexing the results of

[2] "Witting" – a term of intelligence art that indicates that one is not only aware of a fact or piece of information, but also aware of its connection to intelligence activities.

interviews is essential. No intelligence collection discipline is more likely to find meaning in apparently small bits of information than is LINT. Especially when there is reason to have additional interviews with the same individual, the subsequent interviews need careful planning, especially when the interrogator does not speak the language of the person being interviewed.

Intelligence preparation for working in cultures

As with other intelligence collection disciplines, intelligence analysis can play many supporting roles. An obvious one is biographical intelligence, to help identify known hostile undercover personnel, or individuals who will impartially mislead an assortment of national intelligence services for profit.

Equally important is the broader area of cultural intelligence, which draws heavily on the social sciences. In a book review in the CIA professional journal, Lloyd F. Jordan recognizes two forms of study of culture, both of which are relevant to HUMINT. In the review, Jordan describes Patai's book as an excellent example of a second type of cultural analysis. He reviews the first group of scientific analyses of culture and character as beginning with "cultural anthropology as early as the 1920s. During World War II, those methods employed earlier in the academic community in this field of research were brought to bear upon a variety of problems connected with the war effort.

"It was precisely the inaccessibility of the target country and the availability of only fragmentary information about it that made national character research relevant to intelligence analysis during the war. The cultural anthropologists had long been developing models of former and disappearing cultures from fragmentary materials. The anthropologists, joined by the psychiatrists, combined the use of psychoanalytic theory, interaction theory, child development theory, and learning theory with standard anthropological research methods to construct models of the contemporary cultures of wartime enemy countries, Japan and Germany." The classic work of this type is Ruth Benedict's study of Japan, *The Chrysanthemum and the Sword*.

Mike observes that Benedict's approach was the only one in use until the late 1950s. "National character studies" focused on the statistically most significant personality characteristics of the group (i.e., the modal personality), rather than the most common manifestation of the traits. "...modal personality construct[s] tended to be related to the total culture, or at least, its salient features."

The second class of studies, of which Patai's is an exemplar for Arab culture, had a narrower focus. "...they concentrated on the relationship of personality traits to subsets of a given society or a given category of roles of that society, rather than on the identification of relationships between personality and the social structure as a whole." A third category, the comparative study, included Francis L. K. Hsu's *Americans and Chinese*. Indeed, some recent and controversial works, such as Huntington's *The Clash of Civilizations and the Remaking of World Order* can be regarded as an extension of comparative study into the idea of conflicts among the groups compared.

Basic Differentiation by Subject Type

Different types of human subjects will share information voluntarily or involuntarily. The interrogator builds a relationship with the subject, a relationship that can be based on trust, fear, friendship, or any of a range of human emotions. Prisoners have an understandable fear of what may happen, and, contrary to "tough guy" images, it can be important to relax them and, as much as possible, put them at ease. Some organizations teach their members that the other side tortures everyone, and, if that is known, that fear must be addressed; Japanese prisoners in WWII often attempted suicide for that reason but were sometimes dissuaded.

The question of torture should be disposed of at once. Quite apart from moral and legal considerations, (Starfleet would *never* torture anyone)[3] physical torture or extreme mental torture is not an expedient device. "Maltreating a subject is from a strictly practical point of view as short-sighted as whipping a horse to his knees before a thirty-mile ride." The information obtained from torture is likely to be of little intelligence value, and the subject himself is rendered unfit for further exploitation. Physical pressure will often yield a confession, true or false, but what an intelligence interrogation seeks is a continuing flow of information.

Especially when the subject is a prisoner, the screener, who need not be the main interrogator, should examine the Enemy Prisoner of War (EPW) captive tag or other basic information giving the circumstances of capture: when, where, how, by whom, and so forth. If the subject is not under any restraint, it is still quite useful for a screener to prepare contact information comparable to the information on the EPW tag.

When the subject is a POW, screeners should pay particular attention to rank insignia, condition of uniforms and equipment, and behavior demonstrated by the source. Screeners should look for things like attempts to talk to the guards, intentionally joining placement in the wrong segregation group, or any signs of nervousness, anxiety, or fear. Any source whose appearance or behavior indicates that he is willing to talk should be noted by the screeners.

Assuming the subject has been under guard, the screener often can get valuable information about the subject's behavior from the guards. They can tell the screener how the source has responded to orders, what requests have been made by the source, what behavior has been demonstrated by the source, and so forth. Along with the basic contact information, such observations can be extremely helpful to the interrogator, who can study the information before the interview. Having background on the subject helps the interrogator retain the initiative in an interview.

Again for prisoners, screeners should examine the documents captured with the source and any documents pertaining to the source. If the subject is voluntary and providing documents, they may even be more valuable. Screeners may need to get help from linguists or document specialists in understanding the material. If the documents have insignia or other graphics, these should be compared with an existing graphics register, and added to it if they are new.

Documents captured with the source (identification card, letters, map sections, and so forth) can provide information that identifies the source, his organization, his mission, and other personal background (family, knowledge, experience, and so forth). This information can be used to verify information from documents captured with the source and further assess his willingness to cooperate. When examining documents, screeners should look for items that will indicate whether the source is cooperative or willing to cooperate based on any specific personal interest.

If the source has information pertaining to new foreign material, contact appropriate technical intelligence (TECHINT) specialists, and if the source has information of target exploitation interest, contact the appropriate staff members who deal with targeting. These specialists are not necessarily qualified interrogators and may need to meet jointly with the subject and interrogator, or pass questions to the interrogator.

Debriefing

This involves getting cooperating lifeform sources to satisfy intelligence requirements, consistent with the rules, laws, and policies of the Federation, Starfleet, and the STARFLEET

[3] Section 31, which of course does not exist, *might* torture people… but Section 31 doesn't really exist, now does it?

Marine Corps. People being debriefed are usually willing to cooperate, although it is possible to obtain information through casual conversation.[4] Debriefing may be conducted at all echelons and in all operational environments.

Types of people being interviewed include both "tasked" and "non-tasked" individuals. Tasked individuals are, in some way, part of the interviewer's organization.

CATEGORIES OF INTERVIEWEES FOR VOLUNTARY DEBRIEFING

Tasked	Not tasked
Military police and infantry patrols in nominally controlled areas	Residents of nominally controlled areas
Special reconnaissance teams	Nongovernmental organization workers in the area of operations
Diplomats of one's own country	Friendly or neutral foreign diplomats
National or higher command level subject matter experts (*e.g.,* intelligence personnel)	Persons outside the area but knowledgeable about it (*e.g.,* émigrés)

Tasked personnel giving brief reports of the enemy use the SALUTE [5]technique. More formal or extensive debriefing methods are used for obtaining specialized or complex information.

Other than talking to tasked personnel, there is a tendency for some HUMINT collectors to regard debriefing as a waste of time. The approach to a voluntary source needs to be quite different from that to a cooperative prisoner, especially if the interrogator has reason to believe the source is knowledgeable. While a subject may be a volunteer, a refugee or displaced person is likely to have some of the fears and uncertainty undergone by POWs. Active listening and sympathy can pay great benefits, especially in the areas of love of family, and anger at those who made them homeless.

The HUMINT collector should allow specialized or senior sources more latitude to interpose their opinions and evaluations. Prior to the meeting, collectors need to examine all available information, to have an idea of the subject's personality and motivations when beginning to talk to them. It also may require unobtrusive observation of the subject to establish such things as patterns of activity and likes and dislikes. The closer the interview environment can be to the customary surroundings of the subject, the more comfortable and cooperative the source may be.

One example of source that should have latitude are trained foreign internal defense (FID) or unconventional warfare (UW) personnel that work with local residents, or military forces, on a

[4] This actually was attempted on me, in my Navy days, while I was stationed in London. A Russian, who I have always suspected to be a Soviet agent of some kind or another, “taught” me the “right way” to drink vodka in a pub not too far from the USN building and the US Embassy one evening. The end result of that encounter was me filling out form after form regarding the encounter and a long, tedious conversation with Master Chief about it. No fun, but it was fun drinking vodka that a Russian bought for me.

[5] SALUTE is an acronym for Size/Location/Unit/Time/Equipment. **S**ize: how many men in the unit?; **A**ctivity: what are they doing?; **L**ocation: where are they? Give map coordinates if available, otherwise the best description available.; **U**nit: who are they? Uniforms? Descriptions?; **T**ime: when did you see them?; **E**quipment: what weapons do they have? Vehicles? Radios? Anything else distinctive?

routine basis. Such people may very well themselves have LINT and/or counter-intelligence (CI) training; US Special Forces groups have two-man HUMINT/CI teams that can augment operational detachments.

In all cases, the more knowledgeable the interrogator is to the volunteer, the better the result is likely to be. A collector does not need to keep the same level as control as in a hostile interrogation. Sometimes, admitting ignorance of a custom, and respectfully asking for explanation, will trigger a flow of information.

While it takes sophistication, the best general approach to willing subjects is a planned elicitation of information, always with a specific goal in mind. The key to elicitation is the establishment of a rapport between the elicitor and the source, normally based on shared interests. In the initial stages of an elicitation, the collector confines his conversations to innocuous subjects such as sports and social commentary. Dependent on the value of the source, the collection environment, and the security consciousness of the subject, the HUMINT specialist will then shift to a more focused topic.

Once in that mode, elicit the information by continuing to ask for clarification, with questions of the form "I agree, however, what did you mean by....?") or expressing a hypothetical situation. The focused discussion can involve mild flattery and interest in the conversation, or, in a much more delicate approach, selectively challenging statements or introducing new information to show knowledge and stimulate more responses.

Principles of Questioning

The HUMINT collector adopts an appropriate persona based on his appraisal of the source but remains alert for verbal and non-verbal clues that indicate the need for a change in the approach techniques. The amount of time spent on this phase will depend mostly on the probable quantity and value of information the source possesses, the availability of other sources with knowledge on the same topics, and available time. At the initial contact, a businesslike relationship should be maintained. As the source assumes a cooperative attitude, a more relaxed atmosphere may be advantageous. The HUMINT collector must carefully determine which of the various approach techniques to employ.

If a source cooperates, his or her motivations vary. They can range from altruism to personal gain; they may be based on logic or emotion. From a psychological standpoint, the HUMINT collector must be cognizant of the following behaviors. People tend to—

- Want to talk when they are under stress and respond to kindness and understanding during trying circumstances. For example, enemy soldiers who have just been captured have experienced a significant stress-producing episode. The natural inclination is for people to want to talk about this sort of experience. If the Enemy Prisoner of War (EPW) has been properly segregated and silenced, the HUMINT collector will be the first person the EPW has a chance to talk to. This is a powerful tool for the collector to use to get the subject talking. The desire to talk may also be manifested in refugees, DPs, and even local civilians when confronted by an unsettled situation.
- Show deference when confronted by superior authority. This is culturally dependent but in most areas of the world people are used to responding to questions from a variety of government and quasi-government officials.
- Operate within a framework of personal and culturally derived values. People tend to respond positively to individuals who display the same value system and negatively when their core values are challenged.
- Respond to physical and, more importantly, emotional self-interest. This may be as simple as responding to material rewards such as extresponding to support in

rationalizing guilt.

- Fail to apply or remember lessons they may have been taught regarding security if confronted with a disorganized or strange situation.
- Be more willing to discuss a topic about which the HUMINT collector demonstrates identical or related experience or knowledge.
- Appreciate flattery and exoneration from guilt.
- Attach less importance to a topic if it is treated routinely by the HUMINT collector.
- Resent having someone or something they respect belittled, especially by someone they dislike.

BUILDING RAPPORT

"Establish and maintain a rapport between the HUMINT collector and the source. Rapport is a condition established by the HUMINT collector that is characterized by source confidence in the HUMINT collector and a willingness to cooperate with him. This does not necessarily equate to a friendly atmosphere. It means that a relationship is established and maintained that facilitates the collection of information by the HUMINT collector. The HUMINT collector may establish a relationship as superior, equal, or even inferior to the source. The relationship may be based on friendship, mutual gain, or even fear.

If he does introduce himself, normally he will adopt a duty position and rank supportive of the approach strategy selected during the planning and preparation phase. The HUMINT collector must select a rank and duty position that is believable based on the HUMINT collector's age, appearance, and experience. A HUMINT collector may, according to international law, use ruses of war to build rapport with interrogation sources, and this may include posing or "passing himself off" as someone other than a military interrogator. However, the collector must not pose as—

- A doctor, medic, or any other type of medical personnel.
- Any member of the International Committee of the Red Cross (ICRC) or its affiliates. Such a ruse is a violation of treaty obligations.
- A chaplain or clergyman.
- A journalist.
- A member of the civilian government, such as a Member of Parliament.

"The attitude of the interrogators at the preliminary interview should usually be correct, studiously polite, and in some cases even sympathetic. It is imperative that they keep their tempers both now and throughout the interrogation. The prisoner may be given the true reason for his arrest or a false one, or he may be left in doubt, according to the circumstances of the case. The interrogators must try to determine whether his usually vigorous protestations of innocence are genuine or an act, but they should not at this stage give any indication of whether they believe or disbelieve him. A clever prisoner will try to find out how much the interrogators know; they should at all costs remain poker-faced and non-committal.

"At this interview the interrogators should do as little as possible of the talking, however many questions they are anxious to have answered. The prisoner should be asked to tell his story in his own words, describe the circumstances of his arrest, give the history of some period of his life, or explain the details of his occupation. The object is to get him to talk without prompting in as much continuous narrative as possible; the more he talks the better the interrogators can assess his personality.

Recruited/trusted sources

Special Reconnaissance Patrolling

Special reconnaissance is done by soldiers, normally uniformed, who observe enemy activity deep beyond the front line of one's own side. Since these are highly trained specialists, they will usually have been communicating clandestinely to the HUMINT organization, and will be systematically prepared for debriefing. The debriefing may be done by HUMINT officers of their own organization, who are most familiar with their information-gathering techniques. Some of those techniques may be extremely sensitive and held on a need-to-know basis within the special reconnaissance organization. They operate significantly farther than the furthest forward friendly scouting and surveillance units; they may be tens to hundreds of kilometers deeper. They may enter the area of operations in many ways.

Their mission is not to engage in direct combat. It may be to observe and report, or it may include directing air or artillery attacks on enemy positions. If the latter is the case, the patrol still tries to stay covert; the idea is that the enemy obviously knows they are being attacked, but not who is directing fire.

Espionage

Espionage is the collection of information by people either in a position of trust for the enemy, or with access to people with such access. The process of recruiting such individuals and supporting their operations is the HUMINT discipline of agent handling.

It may be possible for an agent handler to meet directly with the agent and debrief him. More commonly, agents send messages to the organization for which they work, by radio, Internet, or by leaving the messages in a hard-to-find place. The latter technique, called a dead drop, will have either a courier or the agent handler retrieve them in a clandestine manner. These are examples of espionage tradecraft.

Analyzing relationships among HUMINT subjects

After interviews, be they debriefings or interrogations, there is likely to be data about other people with whom the subject has had contact or knows about. These data are focused on human relationship networks, not, for example, on military information that the subject knows.

Once information is obtained, it is put into an organized form. Very frequently, information obtained at one interview may help structure the next interview with the same person, or with another subject.

Identifying other people of interest

During interviews, a subject is apt to mention things about other people, or be prompted in a seemingly conversational way.

Operational network "wiring diagram"

Much modern interest in tracking networks of people are relevant to guerilla operations and terrorist networks, two loose categories that do not completely overlap. When examining the overall structure of terrorist groups, there are two general categories of organization: networked and hierarchical. A terrorist group may employ either type or a combination of the two models. Newer groups tend towards organizing or adapting to the possibilities inherent in the network model. Ideology can have an effect on internal organization, with strict Leninist or Maoist groups tending towards centralized control and hierarchical structure. Whether the organizational model is hierarchical or not, the operational personnel almost invariably use the cell system for security.

One relevant study looks at modeling terrorist networks in a manner similar to other systems that "exhibit regularity but not periodicity (i.e., locally random, but globally defined).

Their model focuses at the "mid-range", "not at the level of state leadership, and not at the level of mapping and predicting the behavior of each individual terrorist, but rather at an intermediate or organizational level"... Much as vulnerability analysis of connectionless packet networks such as the Internet concentrates on the nodes whose loss would most interfere with connectivity, the study here looks for the "pattern of connections surrounding a node that allows for wide network reach with minimal direct ties. "Structural holes" at the intersection of flows across knowledge communities position unique and superior nodes. It is the individuals spanning these "internal holes of opportunity" that impact the network's functioning and performance. The implicit corollary of this is that if a small number of these critical nodes can be identified and "clipped" from the network, then command signals will not be able to propagate through the system."

In the 9/11 case, the pilots were such key nodes, once the US operational groups were in-country and operating. Taking the observation of centrality a step farther, COMINT can complement HUMINT in finding the nodes of a geographically dispersed human network.

Obstacles to development of HUMINT capabilities

The following observations are drawn from an article by Lawrence Wright in which he interviewed Director of National Intelligence John Michael McConnell.

Inability to recruit people who are different due to a misperception of security risk factors

To develop HUMINT agents it is necessary to recruit HUMINT controlling officers with native foreign-language skills. However, the U.S. Security clearance process has several problems:

- It is biased against first-generation immigrants with active relationships to their former country.
- It is biased against non-heterosexuals. (For overview see Wikipedia article Sexual orientation and military service.) The U.S. Army, for example, has dismissed hundreds of gays with important language skills, during a time of critical national need for Arabic linguists. This while, according to Wright's article, the FBI has gone from 8 Arabic-speaking agents to 9 in the seven years since the 9/11 attacks.
- It takes up to two years to complete, longer than many immigrants are willing to put their careers on hold while waiting for a clearance.

McConnell's solution to this is to

- Shorten the clearance process to a month or less.
- Subject officers to "'life-cycle monitoring' – that is, constant surveillance".

There have been other cases in the past where it has been necessary to balance security clearance policy against national needs, for example:

- Alan Turing's homosexuality versus Britain's need for cryptanalysis.
- Robert Oppenheimer's radical politics versus US need for nuclear weapons.

DNI McConnell notes also in Wright's article that the predominant risk factor which turns officers into traitors is not ethnicity, sexuality or politics, it is money:

"'Look back at all the spies we've had in our history', he said. 'About a hundred and thirty. How many did it for money? A hundred and twenty-eight.'"

For example,

- Philip Agee allegedly received $1 million from Cuban intelligence service to publicize the names of CIA agents as part of an active measures campaign by the KGB.
- Israel Defense Forces psychiatrist David Shamir "attempted to make contact with the Iranian Foreign Ministry, Hamas officials, and the Russian intelligence service, the FSB, with the intention of selling them classified information which he came upon during his military service". While his claimed motivation was political, the bottom line was still money (emphasis added in quote):
  "Shamir said his prime motivation for his actions was what he viewed as the continued breakdown of the state's social fabric. 'The idea was to save my life and that of my son and the last years of my parents' lives, and to have things happen so that we can really be saved,' he said. '*The thinking was that I would receive money* which I would use to attain asylum for me, my son, and my family, and to enable them to live as reasonably as possible, not in Iran, not in Lebanon, but rather in a European country.' "

Inability to trust people who are different due to failure to innovate in technical OPSEC

Wright claims that "Much of the intelligence community is technophobic and is also hamstrung by security concerns. Only recently have BlackBerrys made their way into some agencies, and many offices don't even have Internet connections." Hence it is difficult to institute technical controls that would allow the organization to effectively compartimentalize the knowledge of officers in the organization so that even moderately untrusted people could serve. I.e., in many cases of "moles" or internal spies, low-level spies have had access to huge volumes of secret data. This would not be possible if adequate technical measures were instituted to effectively compartmentalize information access on a more finely categorized and motivated need-to-know basis. In other words, there is a so far lost opportunity to use technical measures to improve operational security while at the same time allowing a broader range of people to serve. Another aspect of this would be to automatically filter information "down to" and tailored to a specific subject-matter need-to-know characterization of the requesting individual.

Inability to share information across the community due to operational technophobia

A third obstacle to HUMINT and intelligence analysis in general is effective information sharing across the intelligence community. Wright's article notes that "the community still relies on more than thirty online networks and eighty databases, most of which are largely inaccessible to one another". Lack of information sharing has been partly addressed technically by adding new information-sharing tools

Intellipedia, using MediaWiki software with additional security features.

- A-Space, "based on sites such as MySpace and Facebook – in which analysts post their current projects as a way of creating social networks."
- The Library of National Intelligence, which "is an online digest of official reports that will soon provide analysts who use it with tips, much the way Amazon and iTunes offer recommendations to their customers."

However, Wright notes that "These innovations have not yet made their way to the analysts and agents in the field", and "the intelligence community has only warily appropriated models whose usefulness is blindingly obvious".

7.3 Third Platoon: Imagery Intelligence (IMINT)

Third Platoon deals with all aspects of IMINT, gathering and analyzing images from ship's sensors, remote satellites, long-range sensors, drones, aerospace craft, and special sources.

Imagery Analysis is the extraction of useful information from two-dimensional graphic formats. When I was a US Navy Intelligence Specialist, we called it "Photographic Analysis," but the world has technologically matured, and many, if not most, images are now digitally acquired.

Once upon a time, before the invention of photography, military commanders depended on scouts that would survey (recon) enemy activity, depending on simple eyesight and human memory. Perhaps they would sketch what they saw. However, once photography became available, tactical information became frozen in time: details could be preserved and studied, and the quality of available information was enhanced. WWI saw the start of ground-based and aerial photographic collection. Tethered balloons and scout planes were attacked to prevent this information from being collected, and these attacks on observer aircraft led to the development of fighter planes.

The end of the war resulted in the scaling down of tactical and strategic capabilities, resulting in an almost dormant state in the development of photographic analysis. The perceived threat from Germany and Japan revived the collection and analytical capabilities of the major powers, and helped military planners like General D. D. Eisenhower prepare for the next war.

In the 1930s, experiments with film media and its processing resulted in the introduction of film that could now detect non-visible wavelengths in the infra-red (IR) spectrum. Radar made its appearance during WWII, used primarily in its early warning capability. During the early parts of the Cold War, Soviet troops would use a directional radar beacon to lure surveillance aircraft toward their airspace, in order to shoot them down. By this time, radar scopes became available I larger aircraft monitoring Soviet-controlled border areas. Having these scopes made early radar navigation possible; indeed, in photos released by the Soviet Air Force, pictures were taken of the screens, documenting this use.

The importance of tactical information is shown in the case of Operation Market Garden, the aerial invasion of the Netherlands on 17 Sep 1944. Photos revealed the presence of two Panzer divisions in the city of Arnhem, a bridgehead at the farthest reach of those airborne troops assigned. British Intelligence warned the commanders of the threat, but an overpowering optimism caused by the recent collapse of the Western front overruled any possibility of an objective threat assessment. This resulted in a night-time river crossing, in which only 2,600 troops (out of the 10,000 members of the British 1st Airborne Division) would reach the southern shore.

To this day, photo interpreters use black and white film because of the greater detail available. Color film, and digital images in both color and black and white, are also used.

During the early Cold War, the concept of strategic imagery collection was introduced. (In Tactical collection, analysts count guns; strategic collection includes butter.) The categories of collection is, of course, classified. Imagery analysts also use math… it's a common task to determine the volume of storage tanks (that may, for example, hold oil or gasoline) from measurements of the object.

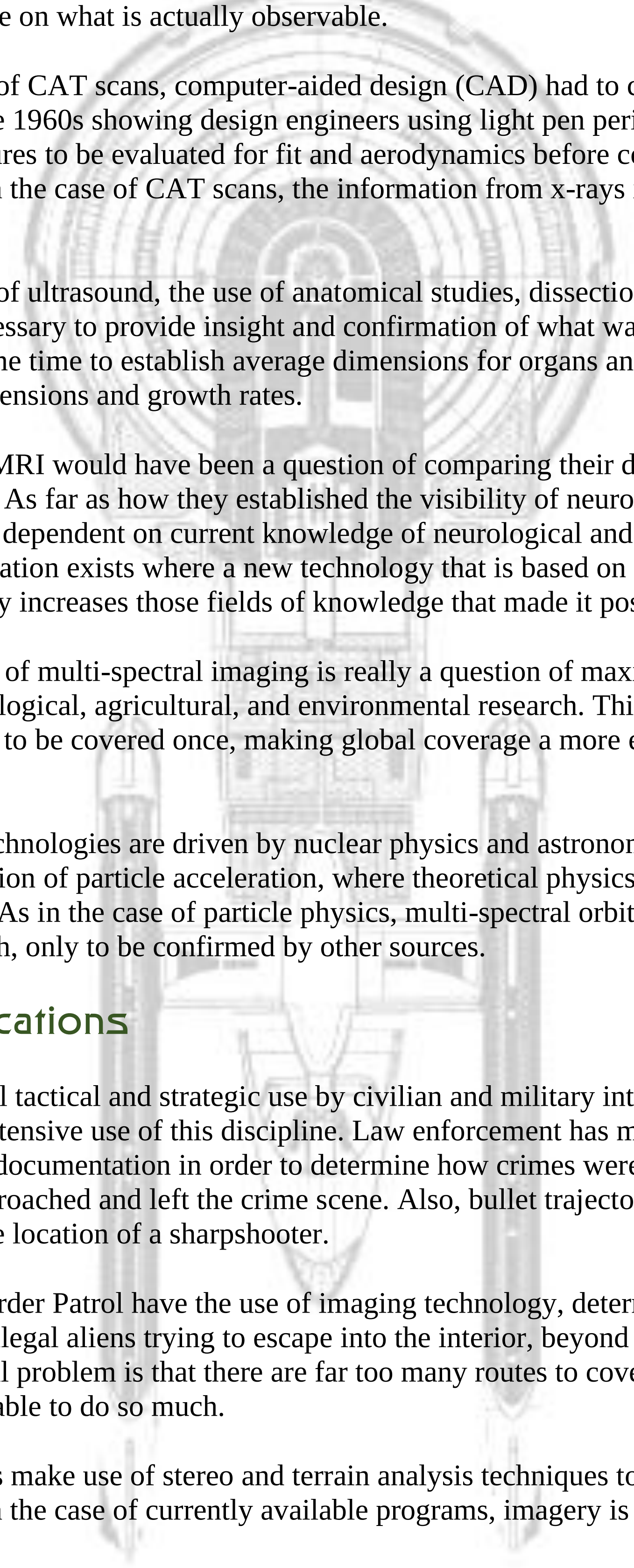
Other techniques have been added to the imagery collection and analysis field: airborne infra-red sensors, synthetic aperture radar, ultrasound (which, in addition to showing variations in tissue density, can be used to detect material flaws in manufacturing), computer assisted imagery analysis (resulting in such technologies as the CAT scan), magnetic resonance imaging (MRI), and multi-spectral imaging (such as the 1970s LandSat).

The first use of tactical imagery obtained during the first World War readily revealed the straight man-made lines of roads, cites, airfields and trenches. Finding concealed high-value targets like artillery, ammo dumps, and other logistical sites was quite another matter.

This was a process that was strictly by trial and error, with the resulting body of knowledge transmitted to new recruits and officers. Terrain and the proximity to supported units would dictate probable locations of logistical routes, ammo dumps, supply depots and assembly areas. Being that the military by definition embraces uniformity, patterns of emplacement and concealment, once discovered would result in widespread targeting by artillery and air strikes. The size, shape, and surroundings of items frequently gave away the location of military assets, with shadows only making it that much easier to identify targets. The development of analytical techniques is really a part of the evaluation of the new technology itself. The first photograph to be taken was that of a French neighborhood. It was crude, yet it clearly showed the outline of the houses. Immediately it was apparent how the new technology, the chemical film plate, was of immediate usefulness.

In the case of infra-red photography, the new details made available were puzzling at first, and took some time to explain. In the pictures taken of works of art, the strange images would eventually be interpreted as showing a feature being painted over and finished. Simultaneous aerial coverage by photo and IR of a given target would reveal how a warm vehicle would warm up the ground and once moved, the warmed plot would stay warm for some time, giving the illusion of more vehicles. Just as in the case of an experienced scientist, once a new observation is made, it must then be explained.

In the case of the application of radar, all there was at the beginning was a variation of the cathode ray tube which would show only the distance to a single target. Only with the introduction of the more familiar round-screen format would radar reach its full potential. So, there were the raw data, but without the use of a readable 2- or 3-D format no-one can make that much use of this information. One thing to remember about radar is that when it comes to illuminating aircraft, most of the energy is deflected. Only the existence of corners, air intakes and flat surfaces that face the radar makes it possible to detect these aircraft. What is actually seen by traffic controllers is the return beep from the aircraft's IFF. As in the case of 9/11, once the hijacked aircraft's IFF was turned off, there wasn't much to see. This can also be seen in the use of radar reflectors that are routinely added to power lines in order to avoid crashes by low-



flying aircraft. The actual characteristics of synthetic aperture radar is of course, classified, so one can only speculate on what is actually observable.

For the development of CAT scans, computer-aided design (CAD) had to come first. Pictures were publicized in the 1960s showing design engineers using light pen peripherals to draw proposed design features to be evaluated for fit and aerodynamics before costly manufacturing jigs had to be built. In the case of CAT scans, the information from x-rays is useless without 3-D capability.

For the development of ultrasound, the use of anatomical studies, dissections, and autopsies would have been necessary to provide insight and confirmation of what was now visible. It would have taken some time to establish average dimensions for organs and, in the case of pre-natal scans, body dimensions and growth rates.

The development of MRI would have been a question of comparing their data with that of CAT scans and ultrasound. As far as how they established the visibility of neurochemical reactions, that would have been dependent on current knowledge of neurological and physiological processes. Now a situation exists where a new technology that is based on previous understanding actually increases those fields of knowledge that made it possible.

The current emphasis of multi-spectral imaging is really a question of maximizing the amount of data available for geological, agricultural, and environmental research. This means that a given area would only have to be covered once, making global coverage a more economical proposition.

The latest imaging technologies are driven by nuclear physics and astronomic research. This can be seen in the evaluation of particle acceleration, where theoretical physics helps to make sense of the collected data. As in the case of particle physics, multi-spectral orbital imaging is driven by theoretical research, only to be confirmed by other sources.

Current applications

Besides the traditional tactical and strategic use by civilian and military intelligence, other entities have made extensive use of this discipline. Law enforcement has made use of imagery in forensic crime scene documentation in order to determine how crimes were committed to include how the assailant approached and left the crime scene. Also, bullet trajectories can be detected in order to determine the location of a sharpshooter.

The United States Border Patrol have the use of imaging technology, determining transit routes and the detection of illegal aliens trying to escape into the interior, beyond the reach of the agents. Their only real problem is that there are far too many routes to cover with the manning and technology only able to do so much.

Highway departments make use of stereo and terrain analysis techniques to determine potential highway routes. As in the case of currently available programs, imagery is included with other types of information to create detailed maps useful for commerce, taxation, city planning, and infrastructure.

The most important application has been for medical and research purposes. Many advances in diagnostics and monitoring have contributed to the ever-increasing body of knowledge and treatment options. The only problem is that with the increase in diagnostic capability, the aspect of accountability and malpractice has made necessary the costly regimen of multiple-discipline testing. This is not about to change. The positive side of developing new imaging technologies is that enhanced observation and understanding will result in better diagnostics and treatments.

The introduction of LandSat in the mid '70s made possible new applications in the fields of agriculture, geology, mining, and the environment. The actual resolution would not be great, but sufficient for these types of applications. The raw data would include the grey scale, and information from a variety of sensors. The designers would find it necessary to assign colors for each type of return, creating a multicolored map.

Meteorological imagery since the '60s has made it possible to detect and monitor severe weather well in advance of its arrival, saving numerous lives.

Future applications

One promising application would be in the field of archaeology. Terrain analysis would show trade routes, lines of communication, cities, forts, farming, grazing, water sources, supporting communities that surround cities and service trade routes, ancient borders, and more.

In the case of Ancient Egypt, IR would reveal water sources that would have supported communities in the desert. Terrain analysis reveals that in order to access the Sinai copper mines, one had to access the shallow eastward valley north of present-day Cairo and reach the Red Sea just south of Port Said. From there it would have been a question of sailing east toward the western coast of the Sinai and turn southward toward Ras Abu Rudeis, a small coastal plain just east of the two copper mines. The reason for this is that an overland route would have required the costly logistical support of garrisons through territory held by hostile desert tribes.

In the case of the biblical Exodus, terrain analysis excludes the traditional sites as being too far and not being accessible to such a large group of people. Advancing through mountainous terrain would have exposed them to ambushes. The only confirmed location within Egypt or the Sinai is that of Baal Zephon. Ancient papyri describe this location as being close to Ramses, Tahpanhes and present-day Lake Menzaleh.

Being that Biblical Archaeology is almost devoid of independent confirmation, one has to use what little confirmed information is available. Following terrain, they would have set out eastward along the Mediterranean coast, reaching the Wadi of Egypt (Al-Arish), and turning southward, following the wadi towards the interior. There are numerous dams crossing the wadi, easily seen from above. Travel would have depended on the use of scouts who would survey water sources, grazing areas and topography that would permit travel for such a large group of people.

Imagery would also benefit exploration in greater Palestine. Radar would readily detect tells (mounds indicative of multiple layers of ruins) in the plains. In mountainous terrain, it would be a question of branching out from confirmed locations and establishing a 10-mile radius, the idea being that cities depend on smaller, surrounding communities. Terrain would dictate probable trade routes, water sources, grazing, farming, and supporting infrastructure.

Surveying jungles would require terrain analysis and radar to detect stone cities and temple complexes.

7.4 Fourth Platoon: Intelligence Analysis and Assessment

Overview

Intelligence analysis is the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context. The descriptions are drawn from what may only be available in the form of deliberately deceptive information; the analyst must correlate the similarities among deceptions and extract a common truth. Although its practice is found in its purest form inside national intelligence agencies, its methods are also applicable in fields such as business intelligence or competitive intelligence.

Intelligence analysis is a way of reducing the ambiguity of highly ambiguous situations. Many analysts prefer the middle-of-the-road explanation, rejecting high or low probability explanations. Analysts may use their own standard of proportionality as to the risk acceptance of the opponent, rejecting that the opponent may take an extreme risk to achieve what the analyst regards as a minor gain. Above all, the analyst must avoid the special cognitive traps for intelligence analysis projecting what she or he wants the opponent to think and using available information to justify that conclusion. To assume that one's enemies try to confuse is not being paranoid but realistic, especially in the areas of intelligence cycle security and its subdiscipline counterintelligence. During World War II the German word for counterintelligence art was *Funkspiel*, or radio game—not a game in the sense of playing fields, but something that draws from game theory and seeks to confuse one's opponents.

Obviously, a set of problem-solving talents are essential for analysts. Since the other side may be hiding their intention, the analyst must be tolerant of ambiguity, of false leads, and of partial information far more fragmentary than faces the experimental scientist. According to Dick Heuer, in an experiment in which analyst behavior was studied, the process is one of incremental refinement: "with test subjects in the experiment demonstrating that initial exposure to blurred stimuli interferes with accurate perception even after more and better information becomes available...the experiment suggests that an analyst who starts observing a potential problem situation at an early and unclear stage is at a disadvantage as compared with others, such as policymakers, whose first exposure may come at a later stage when more and better information is available."

The receipt of information in small increments over time also facilitates assimilation of this information into the analyst's existing views. No one item of information may be sufficient to prompt the analyst to change a previous view. The cumulative message inherent in many pieces of information may be significant but is attenuated when this information is not examined as a whole. The Intelligence Community's review of its performance before the 1973 Yom Kippur War noted [in the only declassified paragraph].

The problem of incremental analysis—especially as it applies to the current intelligence process—was also at work in the period preceding hostilities. Analysts, according to their own accounts, were often proceeding on the basis of the day's take, hastily comparing it with material received the previous day. They then produced in 'assembly line fashion' items which may have reflected perceptive intuition but which [did not] accrue from a systematic consideration of an accumulated body of integrated evidence.

Writers on analysis have suggested reasons why analysts come to incorrect conclusions, by falling into Cognitive traps for intelligence analysis. Without falling into the trap of avoiding decisions by wanting more information, analysts also need to recognize that they always can learn more about the opponent.

Analytic Tradecraft

The body of specific methods for intelligence analysis is generally referred to as **analytic tradecraft**. The academic disciplines examining the art and science of intelligence analysis are most routinely referred to as "Intelligence Studies" and exemplified by institutions such as the Joint Military Intelligence College, University of Pittsburgh Graduate School of Public and International Affairs (Security and Intelligence Studies major), and Mercyhurst College Institute for Intelligence Studies. The goal of the Analytic Tradecraft Notes of the Central Intelligence Agency's **Directorate of Intelligence** (DI) include the

Pursuit of expertise in analytic tradecraft is a central element of this plan. Our tradecraft enables analysts to provide "value-added" to consumers of intelligence by ensuring:

- Dedication to objectivity - tough-minded evaluation of information and explicit defense of judgments - which enhances our credibility with consumers dealing with complex and sensitive policy issues.
- Delivery of our products to the right people in time to be useful in their decision-making and using feedback and tasking from them to drive the collection of the basic intelligence that we need to produce our analysis.

Analytic tradecraft skills also serve as "force multipliers", helping us provide top-quality analysis:

- The feedback our customers give us on our customized analysis clarifies for the analyst what questions most need answering.
- Employing rules for evaluating information and making judgments helps analysts manage the deluge of information, discern trends, and identify attempts at deception.
- Tradecraft standards can be used to iron out differences among experts who have complementary substantive specialties. Their interaction enhances teamwork, which allows the [Directorate of Intelligence] to be more productive.

7.5 Fifth Platoon: Geopolitical Intelligence

In brief, Geopolitical Intelligence is the gathering of information on what is going on, and what is expected to occur, within a geopolitical area.

Geopolitics is the analysis of the geographic influences on power relationships in international relations. The US Navy used the term “Geopolitical Intelligence” to cover this, as well as the gathering and analysis of information regarding the political, financial, and technological situations within a nation, or a group of nations in the same area. For example, when Libya and Chad were at war in the 1980’s, we (the US Navy) spent some time following the developments in that war. Neither country were a direct threat to the United States (although Libyan terrorists abounded), but in gaining and analyzing information on the war – not just the military side of it, but the effects it was having on the two countries populations.

Bringing this into the Star Trek world, the Federation would be studying the behaviors of the various allied and non-allied species, their political situations (did the Ferengi Grand Nagus appoint a new deputy in a ministry dealing with export of machines to press latinum); the geographical changes (The Andorians are terraforming – well, Andoria-forming – a planet at the edge of their space, near a Vulcan science outpost; a Klingon moon just exploded); and other things of that may be of interest (the Tholians have actually retreated from an area of space – something almost unprecedented! Why?)

Other things that would fall into Geopolitical Intel include: Where did “Species X” come from, who are they, and what do they want/lack/need? (The Whale Probe from Star Trek V: The Voyage Home, for example.)

7.6 USMC Intelligence

Now, let’s take a look at the U.S. Marine Corps intelligence field, to give us a bit of historical grounding. As always, remember that WE’RE NOT USMC; we’re a part of a science-fiction fan association.

(*When I was in London, at CINCUSNAVEUR, we had two Marines working with us: a Colonel and a Gunnery Sergeant, in the Imagery section. We squids joked around with them, but they were both sharp, knowledgeable people.)*

This brief is UNCLASSIFIED. (Source: https://en.wikipedia.org/wiki/Marine_Corps_Intelligence)

Marine Corps Intelligence is an element of the United States Intelligence Community. The Director of Intelligence supervises the Intelligence Department of HQMC and is responsible for policy, plans, programming, budgets, and staff supervision of Intelligence and supporting activities within the U.S. Marine Corps as well as supervising the Marine Corps Intelligence Activity (MCIA). The Department supports the Commandant of the Marine Corps (CMC) in his role as a member of the Joint Chiefs of Staff (JCS), represents the service in Joint and Intelligence Community matters, and exercises supervision over the MCIA.

The Department has Service Staff responsibility for Geospatial Intelligence (GEOINT), Advanced Geospatial Intelligence (AGI), Signals Intelligence (SIGINT), Human Intelligence (HUMINT), Counterintelligence (CI), and ensures there is a single synchronized strategy for the development of the Marine Corps Intelligence, Surveillance and Reconnaissance (ISR) Enterprise.

The MCIA, located at Hochmuth Hall, provides tailored intelligence and services to the Marine Corps, other services, and the Intelligence Community based on expeditionary mission profiles in littoral areas. It supports the development of service doctrine, force structure, training and education, and acquisition.

Marine Corps Intelligence Activity (MCIA)

The **Marine Corps Intelligence Activity** (**MCIA**), created in 1987, is a field activity headquarters of the United States Marine Corps, and a member of both the Defense Intelligence Agency and the United States Intelligence Community. The MCIA describes itself as: "a vital part of military intelligence 'corporate enterprise,' and functions in a collegial, effective manner with other service agencies and with the joint intelligence centers of the Joint Chiefs of Staff and Unified Commands."

The Marine Corps Intelligence Activity mission is to provide intelligence services to the Marine Corps and the U.S. Intelligence Community. These services are based on expeditionary mission profiles in littoral areas. It supports the development of service doctrine, force structure, training and education, and acquisition.

MCIA determines what missions the Corps needs to carry out as well as who will need to be trained for that mission. MCIA is in partnership with Marine Corps Intelligence the Office of Naval Intelligence and Office of Coast Guard Intelligence in the National Maritime Intelligence-Integration Office and at Marine Corps Base Quantico in Quantico, Virginia.

Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E)

The MCISR-E is a warfighting enterprise that supports decision-making through the provision of tailored intelligence that is timely, relevant, and predictive. The enterprise supports institutional decision-making through both the provision of relevant intelligence and the comprehensive integration of the intelligence warfighting function in operating concepts, structural decisions, and material investments. The multi-domain, collaborative, worldwide construct of the MCISR-E provides the crucial edge across the spectrum for both deployed and CONUS-based MAGTFs.

What drives the MCISR-E is not the crisis of the moment but rather, the incorporation of a "24/7/365" predictive analysis process with the global reach of operational MEF Intelligence Centers (MICs) backed by the Marine Corps Intelligence Activity (MCIA) and its connectivity to the Combat Support Agencies (CSAs) and National Intelligence Community (IC). To ensure its viability, Marine Corps Intelligence will continue to remain vigilant over a complex, technically sophisticated threat environment and evolve by seizing technological opportunities to increase MCISR-E capabilities and capacities. An intelligent workforce, uniformed and civilian, anchors the MCISR-E with the skills, professional acumen, and functional expertise that mark them as a world-class contributor to our Corps and IC missions.