Gold, Silver, Bronze
Operations Management System

The information in this document is part of the Deltar ‘Level 6 Diploma in Strategic Risk and Crisis Management’
Introduction

The Gold, Silver, Bronze (GSB) command system is used across the world to manage any sort of operation that involves multi-team coordination. Multi-team operations inevitably create issues of command and control, communication, information transfer, and integration with other teams, and possibly other outside organisations. This chapter introduces the basic concepts behind the GSB command system, as well as giving examples of where the GBS system has been used in real-life situations. An understanding of the GBS system will give the security manager the skills to design more complex security operations, safe in the knowledge that they will be able to function effectively and with a high degree of coordination and adaptability in the widest range of possible scenarios.

Gold, Silver, Bronze – Creating Operational Capability

One of the basic problems in security management is turning good ideas into operational capabilities. Unless it is little more than a one-office operation, the likelihood is that the security management operation will consist of various teams, each with their own duties and responsibilities, and which might well be based in different sites, geographical areas, or even countries. The Security Manager will be passing instructions on to other people, often Team Leaders, who will then be expected to carry out those duties. As such, it is likely that there will be the need for a Command and Control Structure that will allow effective daily operations to take place. This module looks at the most common form of Command and Control Structure, and is designed to give the student an understanding of the various components and functions of the system that will allow them to design the most appropriate C&C system for their own organisation.

The three-tiered management structure is common to almost all operational management programmes, whether it is government, military, emergency services or corporate. It consists of Gold, Silver and Bronze Command levels, each of which have their own duties and functions, and it is designed to allow information to pass speedily up the chain, commands and instructions to cascade down the system, and over all a high-level of coordination between the different teams and other units involved in the command structure. If designed correctly, the C & C system should be able to deal equally effectively with standard daily activities, minor incidents that might require immediate response, and crisis management situations that demand a high level of coordination and organisational resilience.

Bronze Command level denotes the lowest level of the command chain, and consists of the people, and teams who will actually do the work. This is often called the Operational Command. This could mean inter-facing with the public, as in a hotel security team, the security teams in an airport or the door supervisors in a pub. The Bronze level teams are the people on the ground, so they will often be the first people who are aware of changes in the immediate situation. As such, as well as carrying out their individual functions, their role is also to be the ears and eyes of the Silver and Gold Commanders, and to pass information up the command chain as required.

Silver Command is the level of command responsible for making sure that that work is carried out effectively, and is often known as the Tactical Command level. Tactical Command could involve defining roles and responsibilities, creating working protocols, delivering training programmes, ensuring that the correct equipment and other resources are in place, and in general ensuring that operational capability is at the required level. The Silver Command level
may well be in charge of a number of Bronze level teams, and one of the functions of the Silver Command is to coordinate the work of the individual bronze teams so that they can respond in the most effective manner to any incident that might occur.

The Gold Command level is responsible for creating the overall strategy, so that each team knows where they fit into the overall command structure, and how their roles contribute to the overall success of any operation.

As an example in a hotel chain, the Gold Commander might be the Regional Security manager, who is responsible for ensuring that there are clear security polices within each hotel, that there is sufficient training and resources to allow the security teams to carry out the functions, and who would review the security operations on a regular basis.

The Silver Commander would be equivalent to the hotel security manager, who is responsible for ensuring that the hotel, its staff, guests and general operations are kept safe, and that all appropriate steps are taken to ensure that those processes are adhered to.

The Silver Commander would also be responsible for managing the response to any situation that would come outside ‘normal daily activities’, such as a complaint from a guest, a report that a member of staff was stealing from rooms, or a tree falling down in the car park. The Bronze Commander would be the person acting as Shift Manager or Team Leader, who would be actively interacting with staff and guests as their first point of contact, and who would be the people actually responsible for the on-going safety and security of the hotel.

Figure 1 The Three-Tiered Security Management System
Almost all security management systems are based on a 3-level management system, Gold (Strategic Management), Silver (Tactical Management) and Bronze (Operational Management)
One of the advantages of the GSB system is that it allows different Bronze Commanders, Silver Commanders or Gold Commanders to coordinate their actions with similar-level commanders in different systems, so as to create effective multi-team working groups. This is the basis of the most ‘senior’ of the GSB Command systems in the UK, COBR, which is the government-level crisis management system. COBR stands for Cabinet Office Briefing Room, and is used when there is the need to coordinate a large number of different organisations for a national crisis, such as terrorism, health scare or natural disaster (such as flooding).

The COBR Strategic Coordinating group is comprised of Gold Commanders of various representative groups, each of which comprises organisations which have their own Gold Commanders. This is an extremely effective system for allowing a large amount of information and expertise to be brought together into one meeting, as well as allowing orders and requests to cascade down the command chain extremely quickly and efficiently.

Figure 3  The UK Government Strategic Coordinating Group Crisis Management System
This example of a Strategic Coordinating group demonstrates the number of stakeholders that need to be included. However, this is an extremely effective way of getting senior decision-makers together, allowing fast decisions to be made that can then be cascaded down through a variety of chains of command.

Potential Problems with the GSB Command Structure

Although the Gold, Silver, Bronze (GSB) Command Structure is recognised as being the most effective way to manage security operations that are bigger than a one-team operation, there are a number of potential problems that are frequently identified as causing problems both in the planning and development stages of security management, as well as in actually responding to incidents.

The first potential problem, and one that is almost always identified as one of the critical causes of operation failure, is Communications. More precisely, it is the failure of the transfer of complex information under pressure. Carl von Clausewitz, the great Prussian strategist, coined the phrase ‘Fog of War’ in 1837 to describe the general chaos and uncertainty that almost always accompanies operational activity. As organisational complexity increases, due to more levels of command and a greater number of different teams, the pressures created by responding to unfamiliar or unknown situations whilst having to operate with less than full information creates an environment where information can be easily lost, misheard or misunderstood.

This can be the case even when the security operation is run by the best trained operation managers in the country. The Jean Charles de Menezes incident in 2005, when an innocent Brazilian student was mistakenly shot by armed police counter terrorism teams, was in a large part due to a misunderstanding as to the nature of the threat. Was it a ‘normal stop’, or was it part of Operation Kratos – a stop with possibility of a ‘critical shot’ to prevent the immediate detonation of a suicide bomber? Despite the clear national threat, and a whole range of briefings, there was still lack of agreement in the report given by one of the officers who made the critical shot, and Commander Cressida Dick, who was acting as Gold Commander at the time, and who had denied giving any order that would have triggered ‘Operation Kratos’. The report into the de Menezes incident by the Independent Police Complaints Commission gives a good insight into some of the issues of command and control in the pressures of immediate incident response.

An associated problem with the transfer of information is stove-piping, or when different departments don’t share information with each other. This can be because there is simply a lack of available channels to exchange information, or can be because different departments see other departments as possible rivals for influence, and therefore see the control of information as a way of maintaining their own power position. This was certainly the case in the run up to 9/11, when the lack of open communication between CIA and FBI (on both an official and informal, personal basis), meant that information that was known and on the record was not shared.

A third problem connected with a hierarchical GSB command system is that often the situation being dealt with demands an immediate response, but the command system means that it takes a long time to transfer information to the decision-makers, who then spend time discussing the situation, and only then start issuing instructions as to how to respond. This is true whether the situation is a national disaster such as Hurricane Katrina or snow blocking UK airports, or a local office complaining that the road to their warehouse is blocked, and they
need to make alternative arrangements. In most cases, the most effective use of the GSB system is to devolve authority to the lowest appropriate level. In other words, if one level of decision maker has the ability to make the decision, there is nothing to be gained by having to go higher up the command chain to receive authority for that decision.

And finally....
As in all security management programmes, the success of the system lies not in drawing pretty command plans with boxes and arrows, but in ensuring that everyone involved in the operation knows what they are doing, understands what they are trying to achieve, and are able to exchange information and make decisions on an on-going basis.

The GSB command System works best when there are three criteria that are met. Firstly, that all of the groups within the system share the same basic culture and ‘risk recognition’. Every security manager knows the frustration from talking with Head Office administrators who don’t understand the seriousness or immediacy of a problem! Secondly, the different people involved in the organisation know each other on a personal basis, and are able to work together effectively for a common cause. And thirdly, that the various teams have worked together in training situations, either with table-top exercises for the team leaders and commanders, or in real-time with the different operational teams.

Summary
As soon as a security management system involves more than a single person, then a Command and Control structure will need to be in to ensure that all aspects of the security management programme are coordinated and controlled in an effective and professional manner. The Command & Control Structure should be able to manage Routine Activities, Minor Incidents and Crisis Situations, and should allow information to be passed up the command chain from front-line responds who have information on any situation and instructions to be passed down the command chain from managers who may well be located far away from the incident site. The ability to create effective command chains is at the heart of effective security management, and it is almost always the case that it is failures in command chain management that is one of the major causes of most security management failures.

Reports