CYBER SECURITY:
CCSS – CLOSE CYBER SECURITY SUPPORT

An accessible way to protect critical information in a tactical environment

Agostino BRUZZONE[(a)] ***Giuseppe GIANNANDREA***[(b)] ***Agatino MURSIA***[(c)] ***Michele TURI***[(d)]

[(a)]University of Genova [(b)] BIGTRES [(c)] Selex Elsag – Catania (Italy) [(d)] UNIGE - DIME PhD course

[(a)] agostino@itim.unige.it [(b)]giannagidgl@libero.it [(c)] agatino.mursia@selex-es.com [(d)]turi@liophant.org

--------------oo0oo-------------

ABSTRACT

Modern military operations are conducted everywhere in the world and soldiers are deployed after a short notice, sometimes with poor training and awareness of the situation on the ground. The channels of communication used are sometimes unconventional, like the Internet, because having quickly available and prerequisite fulfilling communication capability to carry an enormous quantity of information and data is highly important.

One of the main challenges of Cyber Security is to ensure the Confidentiality, Integrity and Availability (CIA) on these channels. However, the threat that cyber operators are facing is like a visible shadow, with no body, that evolves and moves faster than the eye attempting to capture it. This study wants to produce documentation, in order to demonstrate and test through Simulation and C2 systems that a small, well trained and motivated unit on the field, equipped with proper hardware and software, is capable to respond/react on cyber attacks, mitigate them and eventually act and/or react in support of a planned conventional operation.

The necessary support to operations can be obtained with a Close Cyber Security Support (CCSS) capability as or more flexible as the threat to take the opponents engaged in this new terrain as well as in the conventional domains.

INTRODUCTION AND DOCTRINE

The Cyber environment is defined by The Free Dictionary as "The electronic medium of computer networks, in which online communication takes place." The Cyber environment had been recently defined in warfare as the fifth domain coming after Land, Sea, Air, and Space. The Cyber domain from early 21st century is assuming more importance in warfare mainly related to two factors:

- Is a "line" of communication; and,
- Many Command and Control systems are interconnected onto the Cyber domain.

The environment had been developed as a line of communication in order to interconnect computers and provide information in real time. With the continuous development of new protocols of communication, jointed with the improvement of speed and bandwidth, the information achieved a level of quality and accuracy becoming more and more important for the life of individuals.

The information travelling through system interconnected onto the Cyber domain is assuming a strategic importance for the sustainment of nation states in a way that its protection is vital for quality of life. This concept is applicable to systems used daily by individuals, as well as, systems used by military that have the responsibility to serve and protect their country or, in few words, protect the free access and movement through all five domains belonging to their country under its control.

The states concerned in protecting their networks developed organizations with the specific task to protect the asset and provide support to their customers. The intent of this paper is to introduce the concept of a small element or capability applicable in the military environment, such as deployed units, or in crisis where assessment of the situation and immediate responses are required.

The Close Cyber Defence Support (CCDS), applicable in Cyber domain, is drawn from the idea of the close proximity between hostile targets and friendly forces as expressed in the Close Air Support (CAS) doctrine [JP 3-09.3] applicable in the Air domain.

In specific Close Air Support (CAS) operations are conducted in support of and coordinated with ground forces when the distance between friendly forces and enemy targets is reduced to the minimum distance to delineate between the parties during an engagement in combat. An example would be systems designed to maneuver in the Air domain co-operating with systems designed to maneuver in the Land domain.

Taking in due consideration the factor of distance between friendly and enemy parties involved in combat action that motivate the recourse to CAS, the principle of close proximity can be applied in Cyber domain, where distance is no longer a factor of physical separation, but a factor of reachability. This factor is due to a simple consideration that a network of computers that are using the same medium to communicate can be considered as close as next one to another. In other words the modern technology applied to the medium of communication have reduced the distance in a way that the contact between terminals as far as a hundred thousand kilometers apart can be established quickly so that those terminals can exchange large amounts of data in the same way as they are in the same room.

The CAS requires an high level of integration, a flexible and responsive Command and Control structure, a secure line of communication, and a certain number of specialists in order to obtain the maximum effectiveness. These same types of factors that can be applied as well to the CCDS. Moreover, the CCDS can provide the capability of protection for the asset in units or detachments sophisticated enough to provide high level integrated sets of communications over Internet Protocol (IP) systems, where specialists have to provide CIA for the information, and coordination in event a response is needed o emergent attacks.

To support the Cyber domain protection through the deployment of the CCDS capability requires planning in order to accommodate its insertion in the contest, even in the case of insertion while an operation is already underway, the qualified personnel, with specific skills and the required instruments and tools (hardware and software), adapted to accomplish the mission whatever for a short or long duration time period must be available and ready.

APPLICABILITY

The military operations in 21st century are conducted with a peacekeeping or peace-enforcing mandate coming from an international organization, although in some cases a “first strike” condition had forced this organization to approve the new course of action. Troops deployed on the ground early are self-sustaining, establishing the first channel of communication with their mother land. When the operation becomes stable, in time the communication assets start to operate in all cases taking advantage of the “infostructure”, if any are still available, o deployed to the area or the country. At this point, when the channel of communication moves from a secure, internal, and isolated ring, onto a shared and unsecure open worldwide network, the CCDS can better accomplish the mission to protect the information as long as its capabilities and capacities are up to the challenge.

The function of CCDS becomes more important and depends on the mission mandate, in some cases it could be realistic to extend the area of operations widely onto the Cyber domain, in particular if the CCDS is engaged directly from unknown/undeclared entities. However, the course of action of a unit as such typically would have to receive direct guidelines from the highest level of command of the operation. In this case it would will be easy to mediate the attack on the vital support of Intelligence, that can be generate by gathering and crawling information from the Internet, or straight from a service available on the field and mother land.

In fact, even if the CCDS unit is physically kept deployed in proximity of the main gateway serving the Headquarters’ communication node (typically the node connected to the Internet), in case of a targeted cyber attack, the unit can be considered in close proximity to the attacker. This situation, mainly managed directly by specialists and depending case by case, needs a tactic and direction for short time engagements; however, in case the attack develops into a crisis, it may be necessary to receive strategic direction, normally provided by the higher level of command.

CCDS should be able to sustain extended time operations to detect, manage, and respond to security events or incidents in downgraded conditions, and in the case of consolidated situations, the unit could also assume the role of security communication advisor providing its best specific technical knowledge for protection of information. In specific, it should be involved in managing the security of the internal structure of the communication network, concerned in the definition of the different infostructure’s zones, and responsible for the management of all security devices deployed onto the network.

At the very least, CCDS if designed to provide this kind of support, should be able, as well as possibly directed, to accomplish small tactical attack missions mainly in support of the operation or, as part of a bigger asset in direct connection and support with mother land, as larger strategic tasks. With this added capability the CCDS could evolve to a wider concept of Close Cyber Support (CCS).

Because the era of the Cyber space as the fifth domain has opened, the future military Commander is no longer allowed to underestimate the importance to utilize it to pursue tactical and strategic aims, as well as, the utilization of the other domains. The advantage is than to gain and maintain a Cyber superiority through the ability to assure the CIA of the information, and then maneuver within the Cyber domain to compromise and degrade the same ability of the adversaries.

HARDWARE AND SOFTWARE TOOLS

For the CCDS to move from a concept and start becoming a useful tool in the hand of a Commander deployed in operation, necessitates having the resources assigned that in the Cyber domain are mainly hardware and software. In reference to hardware, this document will assume that the reader has knowledge about systems with a Mother Board, Central Processing Units (CPU), Random Access Memory (RAM), Hard Disks (HD), Network Interface Card (NIC), keyboard, mouse and a monitor; in one word a computer or a terminal. However, if for the hardware it is relatively easy to define the components, in definition of the software is much more difficult. One reason is because the large variety of Operative Systems (OS) that is the very basis to allow the terminal work and thus, employ the applications. Another reason is because a tool that makes a specific job or task easier could be available to use with more than one application, and the choice is dependent on operator’s own decision.

To more thoroughly define a CCDS capability through tools and instruments, it is better to start from a software perspective, because the definition of requirements will flow consequently into the hardware acquisition, not forgetting that in many cases certain appliances (the resulting hardware customized and hardened properly for specific tasks) are the best solution.

The Cyber Defense requires firstly a tool where operators and managers can save the information concerning events in a way that once as much information as possible is collected during the management of the event, and once the events are closed, the ability to recall the information when necessary is required. This requirement could be defined as the Incident Management Data Base (IMDB), where a strict Role Based Access Control (RBAC) is employed to allow users, in this case operators and incident managers, to access only the necessary information under the “Need to Know” principle. It is important as well that the IMDB have the capability to share this kind of information in real time among the CCDS components; not only considering that the flow of information could involve external components such as code or malware analysts, forensic investigators and, notably in same case, to the Intelligence community. In this case the information that needs to be shared, because it does not have an assessment or any qualifiers, would have to respect and follow the “Need to Share” principle.

The IMDB could be part, if well developed and hardened, of a larger collaboration suite inclusive of instant messaging application or Voice over Internet Protocol (VoIP), populated with the list of the key personnel to contact on purpose in order to improve the capability to respond to an incident, or help to react as quickly as possible to a crisis, that could compromise the operative status of the infostructure.

The IMDB at the final stage is the main software tool used by an incident handler during the process steps of detection, management, and response to an event or a cyber security incident.

Another tool that Cyber Defense needs to better accomplish its task is a Security Incident and Event Management (SIEM) capability that could be described as the capability to view the infostructure behavior through the analysis and correlation of security events that occur on the network. In brief the eyes of the operator on the flow of digital bits.

A SIEM system is mainly a suite of sensors programmed to read the information flow in bits, and recognizing and capturing those with the intent could be considered as malicious. This process is mainly executed by boxes that in real time are capable to compare the bits of the information flow with an updated database of different specifically behaviors characterizing a malicious code called “signatures”, and in case of positive match, raise an alert or block the flow. Correlated events is the expected outcome of a SIEM. These boxes have names like Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS). The characteristic of a NIDS is to receive packets of bits from a system called TAP that duplicates the information flow for the sensor while leaving it untouched, and they can be used in case there is sufficient information for the organization to receive an alert due to a positive match. As an alternative, the NIPS is inserted directly in the line of communication, without duplication of the information flow, providing the capability to automatically block the malicious code if so configured by the operator. Then the alerts from NIDS or the blocking events from NIPS with logs from systems and events coming from other sources are collected by correlators configured to find a relation, if any, from all these different solicitations and provide a situation alert to the operator.

To deploy a SIEM in an organization depends from the complexity of the infostructure and requires a good plan evaluating the structure itself, the information flow direction, and prioritizing the services that need to be protected by which method.

With these minimum requirements the CCDS can be independent and flexible enough to be deployed in headquarters and organizations where the security of information is vital for the sustainment of the mission assigned, bearing in mind that the main task that a CCDS capability is called to accomplish is coordination among many different information technology actors like system administrators, network managers, web designers, and sometimes skilled users and the systems, without specialists, are useless as a weapon systems without its munitions. Specialists and well trained personnel, with proper equipments, are the key elements for the success of the CCDS capability.

A CCDS PRACTICAL APPLICATION STUDY

The CCDS capability as a relatively small team of specialists, when provided with proper equipments, finds practical application at the level of a peacekeeping or peace-enforcing mission's headquarters, where the main nodes of the Command, Control, Communication and Computers (C4) assets are deployed.

As a descriptive example in this part of the study, a generic military force received a mandate from an international organization to establish peace in a country, fictitiously named BALAVA, at the end of a bloody civil war, with a minimum set of local communications infrastructure still in good conditions. The communication infrastructure had been kept working mainly because it was vital for parties engaged in combat, and it was used to influence the media in reporting their respective points of view to obtain and curry local and international favor. The Cyber space had been massively used during the initial riots that became a civil war through the use, employment and exploitation of Social Networks, Blogs and in some cases, attacks to disrupt specific targets communications even through there is no clear evidence of the source of the disruption.

The military contingent deployed in the country is a Corps composed by soldiers coming from different countries, as an international coalition, with a very specific mandate: establish and support a government capable of leading BALAVA as a united country; create peaceful conditions to resume a normal lifestyle for citizens; and, create the Armed Forces and Police to sustain legality.

The Corps forward headquarters is established in the capital of BALAVA and deploys its communication assets in different phases. Nonetheless in few month the Corps is capable to support the entire contingent deployed in many different towns. Since the early deployment, 70% of the communication assets are computer based, 25% in wideband radio communication and 5% satellite communications. After an initial assessment, that determined that the most important Internet Service Providers (ISPs) are working and providing a bandwidth for the Internet up to 10Gb/s, the decision had been made to take advantage of the infostructure and respectively connect some detached units to the Headquarters via the (Intranet); and, the Headquarters to the Command of the Operation back to mother land via the (Extranet). The satellite link will be used mainly for classified communications (RED) and as backup for unclassified (BLACK) for both Intra and Extranet as demonstrated in figure 1.

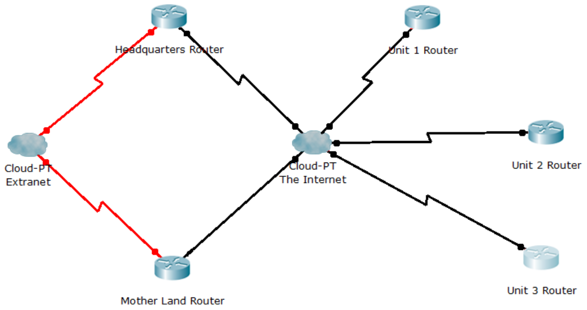

Figure 1 – Example of data link communications

The Cyber space concerning the mission headquarters in BALAVA could cover security events pertaining to both communication channels, the RED and the BLACK. In this case the CCDS capability could be extended to both networks, providing access to operators with the proper clearance; and, will become the Cyber Area of Responsibility (CAR).

Coming back to initial status of the communication infrastructure, likely based on receiving validated Intelligence reports, it is clear that the parties still have a good knowledge of operations in the Cyber space, cyber-operations, and are ready to use it as leverage to gain consensus and/or destabilize the international coalition's interests. Thus with an adequately protected the working environment, a CCDS is capable of providing security of information at the headquarters deployed in the capital of BALAVA, and remotely to all units in the country connected via the Internet, in reason that the Corps, and the dependant units, could be targeted by cyber campaigns of any opposing entity.

The composition of the CCDS team could be as follow:

- One team leader;
- Two sections of Incident handlers;
- One section of code and malware analysts; and,
- One communication section.

The team in total will number ten to twelve people with high technical proficiency specifically in the area of code and malware analysts. However, all of them will contribute to a sort of watchkeeping capability, providing 24/7 coverage, following the security events coming from deployed sensors which are scrolling on monitors, and activating the response team in case of a significant alert.

The team will be endowed with the SIEM capacity, deployed onto the RED and BLACK networks in a way that the team will be able to protect the networks from external and internal intrusions, and maintain the capability to receive the systems' logs coming from e-mail servers, web servers, firewalls, anti-SPAM and anti-virus appliances; and, as much as possible, all core services. The IMDB is available for all components of the team and provides the possibility to share information with J2 Intelligence and J6 operation cells of the Headquarters (HQ). Telephone lines should have the capability to establish a conference call from all regions of the world, and is vital, as a backup line of communication, in case of a crisis where the Internet node might be taken down by Distributed Denial of Service (DDoS) or another kind of cyber attack. As a final capacity the team should have a masked, non-attributed and free from internal control, internet connection, for all the needed intelligence activity that has to be done without attribution utilizing a high capacity World Wide Web access. Nevertheless a sort of small honeypot or honeynet, useful to capture and study a target entity's network behavior is highly desired and needed as well.

The CCDS team, as such, is dependent on the chain of command, from the Deputy Mission Commander, and is appointed as the advisor for cyber security related issues; reporting incidents, and recommending course of actions. A coordination with J6 is necessary for all those activities required to control the mission networks. The Deputy Mission Commander will provide the team the authority to intervene to protect the information and the infostructure in case of attack, or even the worst case of crisis event, to act when decisions need to be taken and immediate actions must take place as quickly as possible. These relationships are partially displayed in figure 2 below.

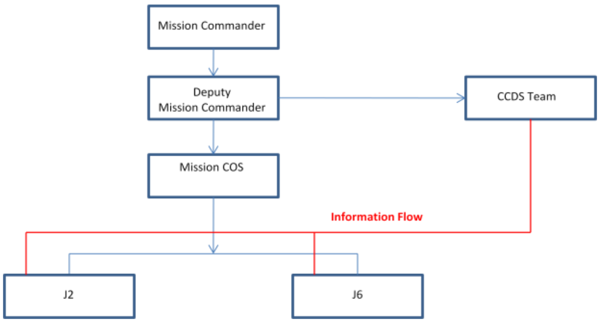

Figure 2 – Example of a chain of command

The primary mission of the CCDS is to provide CIA of the information at the mission's HQ level and below, while taking due consideration that the individual is a preferred target. One of the CCDS's tasks assigned might be to assure the periodic security training of the personnel rotating in theatre. In case of cyber events or incidents that could flow into crimes or espionage, it is important that close collaboration, and eventually a coordinated action with Military Police take place. In other words, the CCDS team is the focal point of all concerns related to the Cyber domain.

CONCLUSIONS

The military, has had been observed in the recent past, to receive very specific care instruction in the Cyber world, particularly from two categories of individuals; activists or "Hacktivists"; and, individuals interested in extracting information likely acting in favor of a foreign Intelligence Service.

In the first category of individuals what is expected is mainly a kind of high media exposure in having taken down military related portals causing a damage in terms of reliability and loss of credibility in attacking what could be considered as unassailable. For these kinds of individuals, it is often enough that the temporary media coverage after the successful event announces their success and attributes their message related to the action. This kind of hacktivist campaign always aimed at the mission’s HQ, thus it is best to leave some of the services, such as Internet portals concerning the mission abroad, associated with a consolidated and well protected environment, likely one existing in well protected national facility.

The individuals that are interested in extracting information, acting mainly through the science of social engineering, run attack campaigns where the main target is the personnel with poor security training, likely human resources or administration personnel. These techniques have the main goal to bypass all of the well applied security measures intended to protect the infostructure. The engineering of the attack maneuver start from a malware affected terminal with a backdoor opened that establishes a direct channel, normally encrypted, with an Internet exposed, and well protected, server called Command and Control (C&C). From this server, via simple commands, the terminal becomes a zombie ready to accept commands and extract data without legitimate user knowledge.

These are the threats that a well prepared and trained CCDS team have to face daily, safeguarding the infostructure potentially under attack from many directions, and where it is important to take care, not only of the equipments and their users, but also provide as much good training as possible to do not let them be the weakest link.