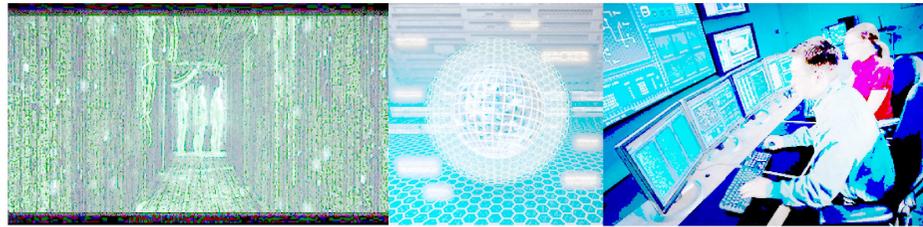




18th ICCRTS

(International Command & Control Research and Technology Symposium)

Institute for Defense Analyses



CCSS – CLOSE CYBER SECURITY SUPPORT

An accessible way to protect critical information in a tactical environment

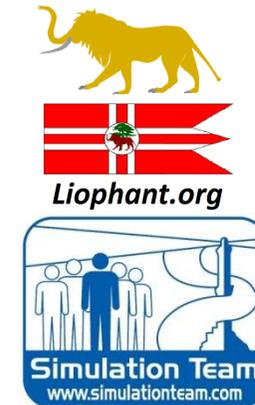
Prof. Agostino Bruzzone
Genova University
Network
agostino@itim.unige.it

Mr. Giuseppe Giannandrea
BIGTRES NETWORK
giannagidgl@libero.it

Mr. Agatino Mursia
Selex ES Spa
agatino.mursia@selex-es.com

Dr. Michele Turi
DIME (PhD Program)/BIGTRES
turi@liophant.org

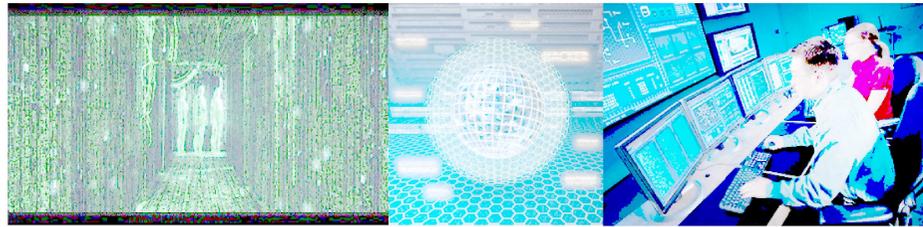
(June 19-21, 2013) Alexandria, Virginia (US)



18th ICCRTS

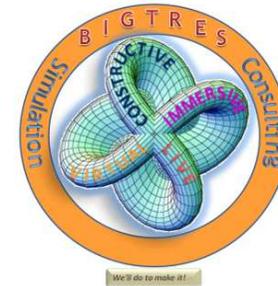
(International Command & Control Research and Technology Symposium)

Institute for Defense Analyses



AGENDA:

- INTRODUCTION & DOCTRINE
- CONCEPT
- APPLICABILITY
- HW & SW TOOLS
- PRATICAL APPLICATION
- CONCLUSIONS



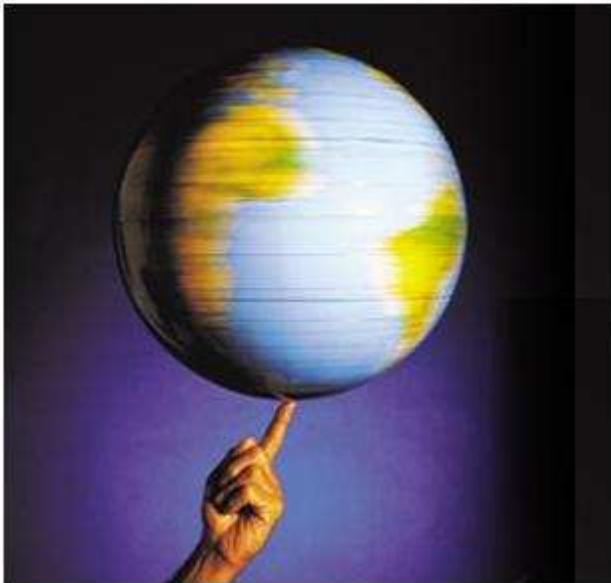
UNIGE - D.I.M.E.



Liophant.org



The Cyber environment had been recently defined in warfare as the fifth domain coming after Land, Sea, Air, and Space.



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.

CONCEPT

The Close Cyber Defense 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.



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.

The military operations in 21st century are conducted with a peacekeeping or peace-enforcing mandate.

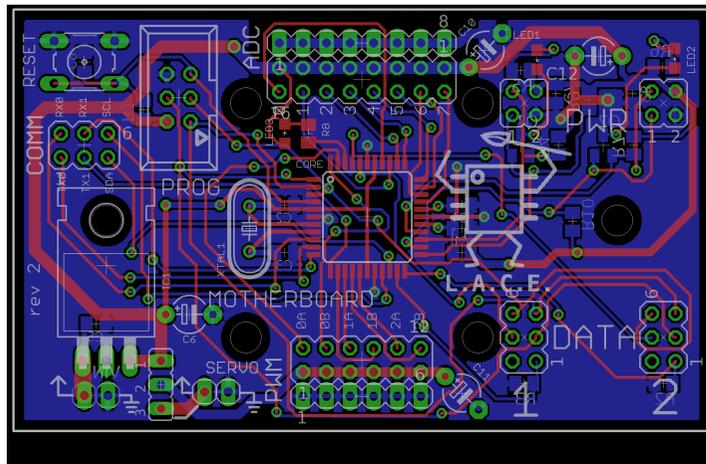
Troops deployed on the ground early are self-sustaining, establishing the first channel of communication with their mother land.

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.



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. (The front line)

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.



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.



Another tool that Cyber Defense needs to better accomplish its task is a Security Incident and Event Management (SIEM) capability

SIEM described how to view the info-structure behavior through the analysis and correlation of security events that occur on the network.



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.



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.

If 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.



Since the early deployment, 70% of the communication assets are computer based, 25% in wideband radio communication and 5% satellite communications.

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).

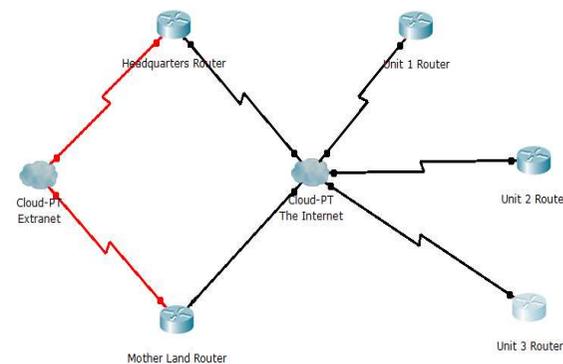


If required all of them will contribute to a sort of watchkeeping capability, providing 24/7 coverage, following the security events coming from deployed sensors.

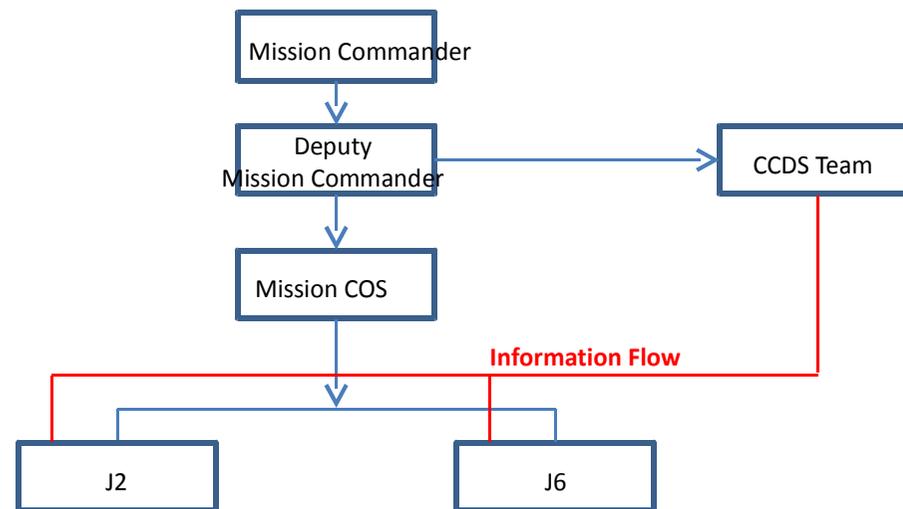
The composition of the CCDS team could be as follow:

- 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.



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.



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.

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”

individuals interested in extracting information likely acting in favor of a foreign Intelligence Service.

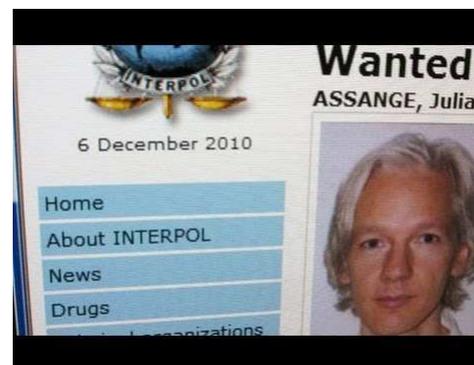


CONCLUSIONS

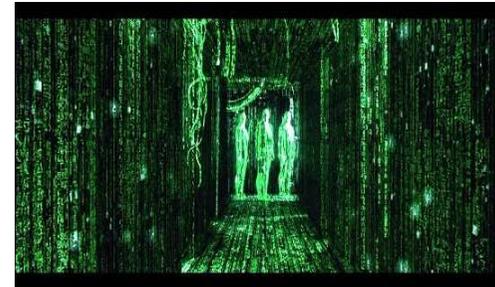


In the first category of individuals what is expected is mainly a kind of high media exposure.

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



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.



Questions?

