IST-152 Workshop on Intelligent Autonomous Agents for Cyber Defense and Resilience

Perspectives on Autonomous Intelligent Multi Agent Systems for the Cyber Defense of Military Systems. A case study.

Paul THERON[1]

Submitted in July 2017

SUMMARY

While Multi Agent Systems (MAS) have been around for three decades now, cyber defense (and resilience) on the battlefield poses new challenges: Stealth and isolated combat systems, the Military Internet of Things and human operators who being defense specialists are not cybersecurity geeks, and shouldn't be bothered by cyber-incident response. The first two contexts require an alternative to classic probe / SIEM / SOC solutions. These contexts and domain-specific requirements and constraints influence the architecture of cyber defense solutions for the battlefield. This paper, based on an operational use case, reviews first the cybersecurity context and specificities of the modern battlefield, including a review of the evolution of the cyber-threat. Next, it sketches briefly the concept of Multi Agent System to introduce it in the military context. Its third part describes the use case studied in the context of IST 152's RTG. Taking the example of a Ground-Air Defense system, it shows that three options are available for deploying Multi Agent Systems for the Cyber defense of military systems. Finally, introducing IST 152 RTG's MASC (Multi Agent System for Cyber defense) Reference Architecture, we argue that it represents a valuable short-term solution within the frame of operational constraints previously exposed. We conclude that the feasibility of using Multi Agent System technologies for cyber defense still depends on a vast program of research.

BACKGROUND CONSIDERATIONS ON CYBER-ATTACK STRATEGIES: EXAMPLE OF AIR FORCES

In the case of Air Forces, for instance, the RAF affirms in the "*Future Air and Space Operational Concept in Practice*"[2] document that *"The air power contribution to future operations is underpinned by a robust, networked air command and control system, populated by air-minded officers, that is resilient to cyber-attack, counter-ISTAR information and conventional attack*".

Alas, already cyber-attacks have grounded military aircrafts and air operations can be jeopardized, or supported, by the right moves in the cyberspace.

The Aviationist website[3] reports on February 13th, 2009 that French Navy's Rafales were grounded by the Conficker worm virus in October 2008, raising the issue of systems' maintenance. A Thales Raytheon marketing leaflet[4] highlights the risk of Denials of Service targeting Air C4I systems or civilian ATM systems. On November 6th, 2007 Israeli fighter jets bombarded the Syrian Dayr-az-Zawr

---

[1] Mobile: +33 6 86 65 20 81 – Email: paul.theron@thalesgroup.com; Member of NATO's IST 152 Technology Research Group; Co-Director of the "Aerospace Cyber Resilience" research chair (https://www.linkedin.com/company-beta/11211070/ and http://www.crea.air.defense.gouv.fr/index.php/chaire-cybair)

[2] http://www.raf.mod.uk/rafcms/mediafiles/62873A71_C94D_D318_DC50FF8024A36D04.pdf

[3] https://theaviationist.com/2009/02/13/french-navy-rafales-grounded-bya-computer-virus/

[4] http://www.thalesraytheon.com/fileadmin/tmpl/Products/pdf/Cyber_Security/brochure_CYBAIR_EXE_low.pdf

nuclear plant after Syria's air defense network and its radars in particular had been previously disabled by a targeted cyber-attack. In 2009, $26 Skygrabber software plus a satellite dish allowed to access the video traffic generated by a Predator drone. On October 2011, Wired magazine reported[5] that a virus could capture strokes on drone cockpits keyboards at Creech Air Force Base in Nevada, making it tricky for pilots to remotely fly Predator and Reaper assault drones. And (RT.com, 2011) adds that for Sergey Novikov, the head of Kaspersky's EEMEA research center, this was "*not a targeted attack [but] a simple Trojan, which infected the network of this military [base] in the US*".

Cyber-attacks target also non-military aviation assets.

In the USA, at the Defcon 20 conference of July 2012, a hacker named Brad "RenderMan" Haines presented how to attack the ADS-B due to the precarious design of the GPS. On September 12th, 2011 NewScientist reported a fictional cyber-attack scenario in which corrupted ADS-B data would lead an aircraft pilot to believe an imminent in flight collision was to happen, inducing his decision to dive down only to collide effectively with aircrafts present in a crowded lower air lane.

On August 29th, 2014, abcNEWS reported that spoofing radio communications between ATC and aircrafts was an increasing problem with "*three such incidents there in 1998, 18 last year, and now, so far this year, 20*" and that hackers had given false instructions to pilots or broadcasted fake distress calls for instance.

Civil Air Traffic Management, a regular co-operator in military air traffic, can also be the target of cyber-attacks. (CANSO, 2014) states that the cyber threat is "*both very real and very serious*", and so does the UK's Centre for the Protection of National Infrastructures (CPNI UK) in a report[6] released in August 2012, or, in 2009, the US Department of Transportation audit report[7] that revealed that almost 4,000 vulnerabilities had been found in FAA's computer systems, of which 763 classified ones allowing attackers to take control of computers, to modify and to steal data, while it acknowledged that in 2008 the FAA got 800 cyber-attack alerts, including malicious server breakdowns and unauthorized access to 48,000 employees' data.

The Telegraph reported a supposedly "*Chinese" attack against "Officials at Malaysia's National Security Council and Civil Aviation Department*" who were among those involved in the hunt for missing flight MH370. Dr Amirudin Abdul Wahab, the head of Cyber-security Malaysia, said "*the hackers succeeded in stealing significant amounts of information*", including "*minutes of meetings and classified documents […] some of these [being] related to the MH370 investigation*". According to him, "*It was a very sophisticated attack*". This case depicts the capacity of attackers either to plan ahead of events for attacks they might wish to carry out, or to mount attacks very quickly as might have been the case here.

Data leaks may also happen "*by mistake*". Sunday Express reported on June 13th, 2014 that this is what happened on June 5th and June 10th in the European sky when air-traffic controllers in Austria, Germany, the Czech Republic and Slovakia realized that data about planes' position, direction, height or speed had suddenly gone missing. The incident was blamed on a military cyber warfare exercise, possibly run by NATO it was said, that would have interfered with ATM systems.

---

[5] https://www.wired.com/2011/10/military-not-quite-sure-how-drone-cockpits-got-infected/

[6] http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf?epslanguage=en-gb

[7] http://www.pcworld.com/article/164501/article.html and http://www.nbcnews.com/id/30602242/ns/technology_and_science-security/t/air-traffic-systems-vulnerable-cyber-attack/#.VCgDdqz0u7h

Civilian air traffic can also be grounded by cyber-attacks. SiliconRepublic reports[8] that on 21st June, 2015 Polish air traffic was grounded after a cyber-attack stopped Polish company LOT flying ten aircrafts out of Chopin Airport in Warsaw. Forbes website[9] also reports on April 16th, 2013 that American Airlines struggled to regain control of its computer systems and that almost 2,000 of the company's daily flights had been cancelled or delayed due to an unspecified computer system outage.

In this context, actions have started being taken in the past ten years (US Air Force, 2008). Currently, still in the USA[10], SiCore Technologies Inc., Farmingdale, New York, and Ball Aerospace & Technologies Corp., Boulder, Colorado, have been awarded $ 95.800.000 Air Force-related cybersecurity contracts by the US Department of Defense. The latter has also published its cyber strategy[11] that seeks to defend DoD networks, systems and information, to defend the U.S. homeland and U.S. national interests against cyber-attacks of significant consequence, and to provide cyber support to military operational and contingency plans with by 2018 the support of a 133 teams strong Cyber Mission Force. Every country around the World is now investing on aerospace cybersecurity, for example in France with the creation of the Aerospace Cyber Resilience research chair[12]. NATO has launched a number of initiatives, such as the IST 152 RTG and others, in the wider domain of military cybersecurity and cyber defense. In the EU, the SESAR Joint Undertaking has performed studies and launched projects to tackle cyber-risks.

THE EVOLUTION IN TIME OF CYBER-ATTACKS

Retrospectively, over the past thirty years or so, cyber-attacks look like a succession of tests designed to evaluate the vulnerability of target systems, cyber-attack strategies, attack patterns and cyber-defense systems' effectiveness.

(VENAFI, 2013) states that attacks become more and more intelligent and have now reached a kind of *first-generation* technical climax.

Beginning around 1995, the first cyber-attacks used viruses or worms and targeted whatever server or workstation they could replicate onto. They often aimed at making their authors famous or at making claims for a cause. In 1998, the CIH virus infected more than 60 million computers to challenge the antivirus industry's claim of efficiency. Around year 2000, (Distributed) Denial of Service ((D)DoS) attacks sought to disrupt ICT systems including the Internet itself. The 2003 Slammer worm infected 75,000 computers and slowed down the Internet traffic. By mid-2000, cybercrime became dominant, aiming at money extortion or to turn individual PCs into relays of wider botnets (like Mydoom in 2004). Today ransomware prolongs this criminal trend. Cyber-espionage and data exfiltration became common in late 2000's. Stealing bank account data happened as early as 2007 with the Zeus Trojan malware. In 2008, it is said that the Conficker malware infected millions of governmental servers and workstations in nearly 200 countries across the world. In 2010, Stuxnet infected Iranian nuclear plants' industrial systems by compromising digital certificates and using 'zero-day exploits' to propagate itself to the target systems its authors wanted to disrupt. Staff

[8] https://www.siliconrepublic.com/enterprise/polish-air-traffic-grounded-after-cyber-attack
[9] http://www.forbes.com/sites/brighammccown/2013/04/16/american-airlines-grounded-accident-of-cyber-attack/#15ce90e56c9e
[10] US Department of Defense, Release No: CR-059-16, March 30, 2016, at http://www.defense.gov/News/Contracts/Contract-View/Article/708805
[11] http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy
[12] http://www.crea.air.defense.gouv.fr/index.php/chaire-cybair

introduced the malware into a USB port of the plant's computers. Stuxnet was perhaps the first attack designed to cross 'air gaps' between systems. In 2011, the Diginotar malware took control of the eight trusted certificate-issuing servers of a Certificate Authority, forcing them to declare themselves untrustworthy to the government and business clients. In 2012, the Flame malware intercepted requests by IT servers for software updates and forged Microsoft certificates to deliver malicious programs to users. In May 2017, the WannaCry ransomware cyber-attack is said to have affected more than 230.000 computers. The fruit of a fairly basic, wide ranging attack strategy, its knock-on effects were important, paralyzing hospitals in the UK, car manufacturer plants, etc.

Some key trends can be drawn from this retrospect:

- Cyber-attacks have increased in number and the cyber threat is today's "new normal";
- Attackers' goals are increasingly ambitious; they tend to multiply attack vectors and targets and to continuously increase the sophistication and diversity of their attacks;
- They attack cyber defense mechanisms themselves to perpetrate in-depth attacks;
- Low-key wide-ranging attack strategies may generate severe systemic impacts;
- Attack technologies have improved from simple programs overriding systems' functionalities, to scripted pervasive software capable of replication and designed to take control of systems' security privilege management functions, and finally to remotely controlled software agents that can be activated by a Command & Control server itself masked behind layers of camouflage false IP addresses and routes;
- This "new normal" creates a climate of permanent uncertainty and distrust both in systems and societal forces, and even in people operating or simply using systems;
- As technology makes progress, attack technologies will progress again. (Guarino, 2013) reports that Autonomous Intelligent Agents for cyber-attacks are already being developed to defeat current cyber-defense technologies and to increase attackers' strike power.

BUILDING THE CASE STUDY: INFLUENTIAL SPECIFICITIES OF OPERATIONAL DEFENSE SYSTEMS

Military systems currently pose five crucial challenges:

1- Stealth and isolated combat systems, effectors, should embed autonomous cyber defense solutions as there have no way to connect to a SOC. Either effectors are small or unmanned devices, like drones, and cannot embed a SOC-like cyber defense system, or they are large, like a sea vessel, and there may be an onboard SOC, however often with a limited team of cybersecurity specialists. In both cases, the best option is probably to embed in them some form of autonomous cyber defense mechanisms doing the job for humans.

2- The future Military Internet of Things is in line with the doctrine of high connectivity providing information superiority. But it raises the question of the cyber resilience of complex and massively distributed and interconnected systems. Its cyber defense will have to be as distributed as the system itself, and the autonomy of cyber defense mechanisms might soon appear to be necessary in conjunction with the stealth and disconnection challenge.

3- Finally, military human operators are defense specialists, not cybersecurity geeks. They should not be bothered by cyber-incident response duties. Otherwise, the risks of mental overload and distraction ultimately compromising missions' success are assumed to be too high.

The first two contexts require an alternative to classic probe / SIEM / SOC solutions. The third context requires embedded cyber defense capabilities in order to discharge humans of the cyber-attack reaction burden.

4- Data and systems' classification

The battlefield involves both decentralized and global, theatre-wide, operations and commandment. Defense systems, from headquarters to the tactical level, spread over a variety of locations while some of their data or equipment is classified while others are not, requesting the physical segregation of means, people and premises.

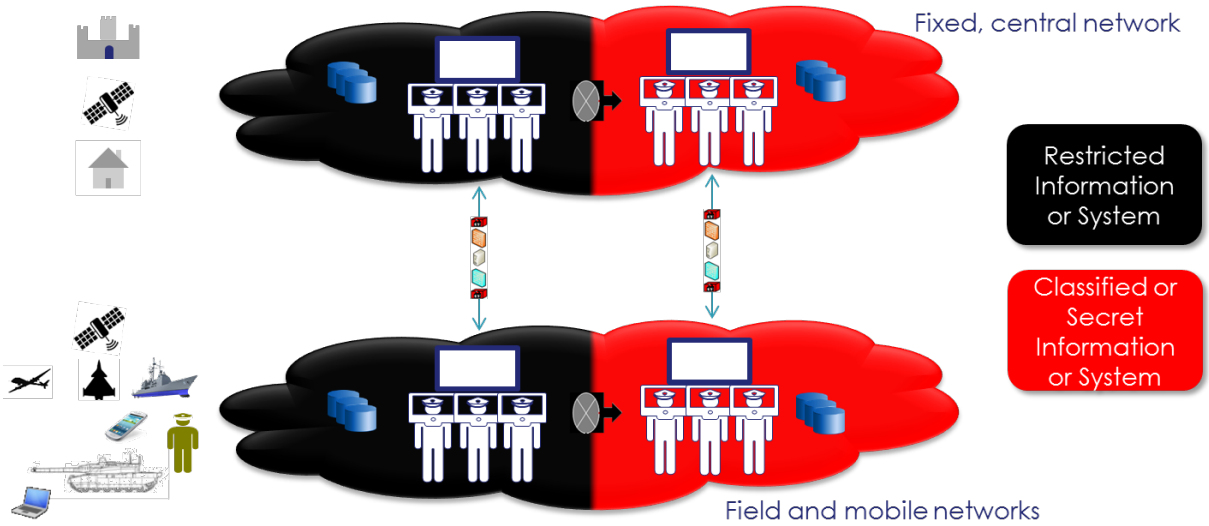

Figure 1 A broad view of classification-related segregation in military systems

The less secret systems are, the more likely they are to be connected and open through access networks that include them into wider defense networks. The more secret, the more autonomous they will be, which does not mean that they are not connected, only that they are part of classified networks that themselves are segregated from non-classified networks.

Differences in classification levels impact on cyber defense architecture. Classified systems need a cyber-defense of their own. So, at least two cyber defense systems have to coexist within a single force. Cyber Defense solutions have to be designed, implemented and operated in this strict cadre.

5- Types and generations of technologies

Different generations of defense systems coexist within forces and coalitions. Older generations cannot be secured like future ones. Their design never embarked cybersecurity into their genes and contractual warrantees and technical support often exclude any modification or addition of a tap here or a firewall there (not mentioning an autonomous intelligent multi agent system).

The "age" and type of a piece of equipment have a direct impact on the possibility and way of its cybersecurity. Five different types of defense equipment can be identified:

- Office and information management systems (handling for instance, human resources, logistics, messaging or… big data computation these days);

- C4ISR systems for battle commandment (including their extension, battle management systems used on the ground);

- Communication systems (satcom, tactical and line of sight for instance are good examples, and one could add combat clouds…);

- Platform and life automation systems such as those found onboard ships and vehicles or within ground premises (this includes for instance air conditioning systems, lifts, apparels used for handling stocks or maintaining combat systems, etc.);

- Effectors, i.e. weapon systems and other equipment (this ranges from rifles to jet fighters, from radar stations to tanks, etc.).

Figure 2 Five types of military systems

The first three types are rather classic IT systems and all cyber technologies and good practices that apply to IT can potentially apply to them, beyond classification issues and a few specificities.

But the last two types belong more in the OT family, operational technologies, that were designed with only functionality, performance and reliability in mind. Their solutions and architectures are specific. Their performance, on the battleground, depends upon their correct use, by the manual, so that the addition by users of cybersecurity features and devices is very likely to be contractually discouraged as it triggers unacceptable risks of failure.

The cyber defense of military systems will be essentially peripheral and probably only physical for the oldest generations of equipment. New and future equipment may be added cyber defense mechanisms or will be specified to embed them.

MULTI AGENT SYSTEMS FOR CYBER DEFENSE

For (Talukdar, 1999) an autonomous software agent is "*any encapsulated piece of computer code, such as a program or a subroutine*" that can be modeled as "*a set of computer-maintained memories from which the agent can read (the agent's input space), a set of computer-maintained memories to which the agent can write (the agent's output space), an operator embodying the agent's problem-solving skills that can copy objects from the input memories, transform them, and write the results to one or more of the output memories, and a control system consisting of the agent's own social skills together with any external controls, such as reporting requirements, imposed by the organization*". And it is autonomous (ibid) "*if its control system is completely self-contained, that is, if its social skills are its only controls. As such, an autonomous cyber agent can do what it wants when it wants*" and

its "*work cycle*" consists of "*the following sequence: read (copy) a set of objects from its input-memories, modify these objects, and write the results to one or more of its output-memories*".

An agent has sensors and effectors and it can communicate with the external world while it has the embedded capacities needed to perform its tasks. It makes choices between options, for instance on the basis of a utility function (Neumann & Morgenstern, 1944).

Multi Agent Systems (MAS) are made of a set of individual agents (Jamont, 2016). Its multiple agents, while acting locally on the basis of their individual knowledge and rules, cooperate together towards a common goal, which requires some form of collective intelligence. They are close to naturalistic behaviors such as ants' and bees', their connectivity is in line with the doctrine of information superiority through high connectedness, their versatility implies a vast number of configurations and functions for a wide variety of issues, they help the decentralization, distribution and sharing of resources and decisions.

In this context, what Autonomous Intelligent Multi Agent Systems for the cyber defense of military platforms will need to do in the future is vast, in terms of both functional and application scope.

RAND's recent report (Snyder, et al., 2015) and (Gowing & Langdon, 2015) point out the need for both cybersecurity and cyber defense. Cybersecurity and cyber defense together form cyber resilience (Theron, 2013). Cybersecurity seeks to avoid cyber-attacks and other ingenuous cyber-incidents. Cyber defense seeks to cope with those cyber-attacks and other ingenuous incidents that happen despite cybersecurity measures. Cyber resilience engineering seeks to fit into target systems the mechanisms and techniques (Bodeau & Graubart, 2013) that help both to prevent attacks and to respond to them.

The functional scope of MAS technologies should be cyber defense. In (Bodeau & Graubart, 2011), this corresponds to the Withstand and Recover goals, to the Detect and Respond functions in (NIST, 2014), to the Recognition and Response mechanisms in (Theron, 2013).

An Autonomous Intelligent Multi Agent System for Cyber Defense could be defined in a first approach (Théron, 2016) as:

- A set of software or hardware (possibly human) entities (Sensors, actuators, repositories, cyphers, transmitters, cognitive functions, human collaborators)…
- Embedding their own methods, policies, self-management capabilities, resources, energy-generation features and capacities for hiding, detecting and understanding attacks and their various signals, devising reaction plans, keeping Situation Awareness for sense making and changing / optimizing reaction plans when and as circumstances require, using local / distributed resources to perform or optimize tasks, collaborating with human operators as and if needed, and learning and improving their own capabilities…
- Interacting through rules and methods, interfaces, communication and cooperation protocols, discovery and invocation procedures, runtime enablers…
- Creating collectively the intelligence (i.e. not just exchanging data but building together emerging capabilities) required to carry out cyber defense missions, to adjust their goals and make decisions and choices while these missions, goals and decisions cannot be pre-programmed and need to be dynamically elaborated on the basis of contextual elements…
- According to set of *ad hoc* policies, either administrator-defined, or devised or optimized according to actions and circumstances.

Besides, it should be stealth and, more generally speaking, cyber-resilient itself, trustworthy, and energy-saving.

From an application scope standpoint, (EMAA, 2013), for instance, identifies the components of Air Defense systems, beside effectors, that require to be protected:

- Data,
- Support networks,
- Applications,
- SCADA, and IACS[13] more generally.

But "*Many of these information systems lie outside U.S. Air Force control because they were made by foreign firms or are under the management of commercial firms or foreign entities*" (Snyder, et al., 2015).

These considerations raise two requirements for Autonomous Intelligent Multi Agent Systems for Cyber Defense:

1. They should be embedded in every single of these components, the issue being how to do this, and without affecting the performances of military systems;
2. Engineering should be perfectly controlled, both of the Autonomous Intelligent Multi Agent Systems for Cyber Defense and of the military systems due to embed them into their architecture and functionalities.

THE USE CASE AND CONOPS

Assuming that the five types of military systems described in Figure 2 may be supervised by a central Cyber-C2, a Security Operations Center (SOC) providing the commandment with a consolidated cyber picture of the battlefield, we hypothesized that the overall architecture could be as follows:

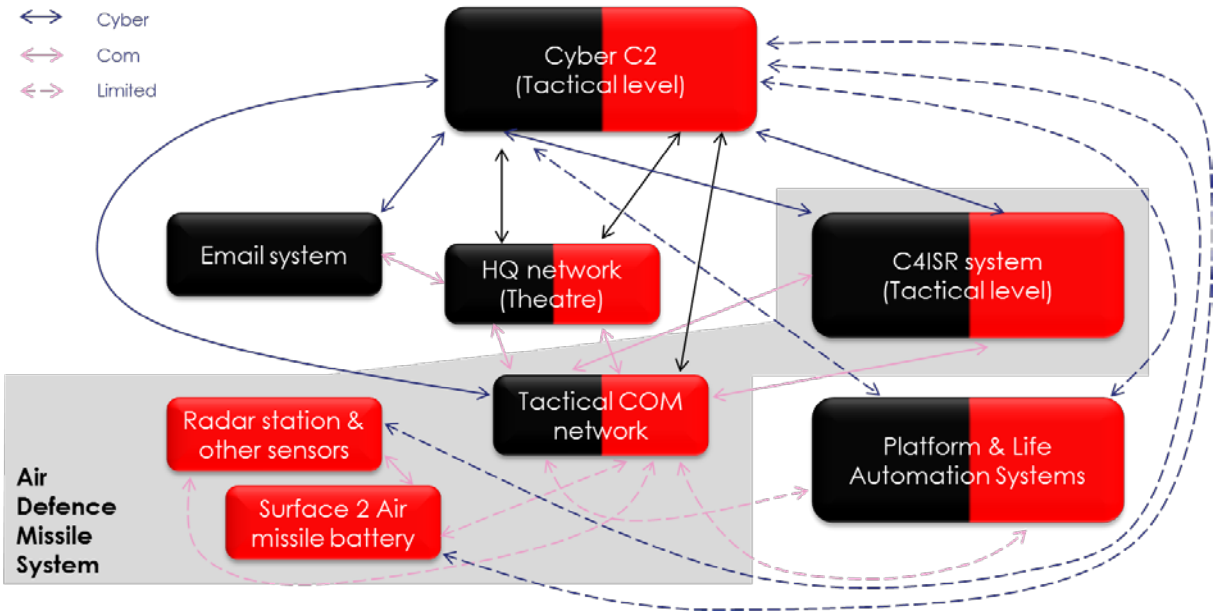

Figure 3 Example of military system (dotted lines indicate possible disconnections of systems)

[13] See IEC 62443 standard suite for a definition of Industrial Automation & Control Systems

A simple implementation of cyber defense mechanisms across this architecture would look like, for instance:

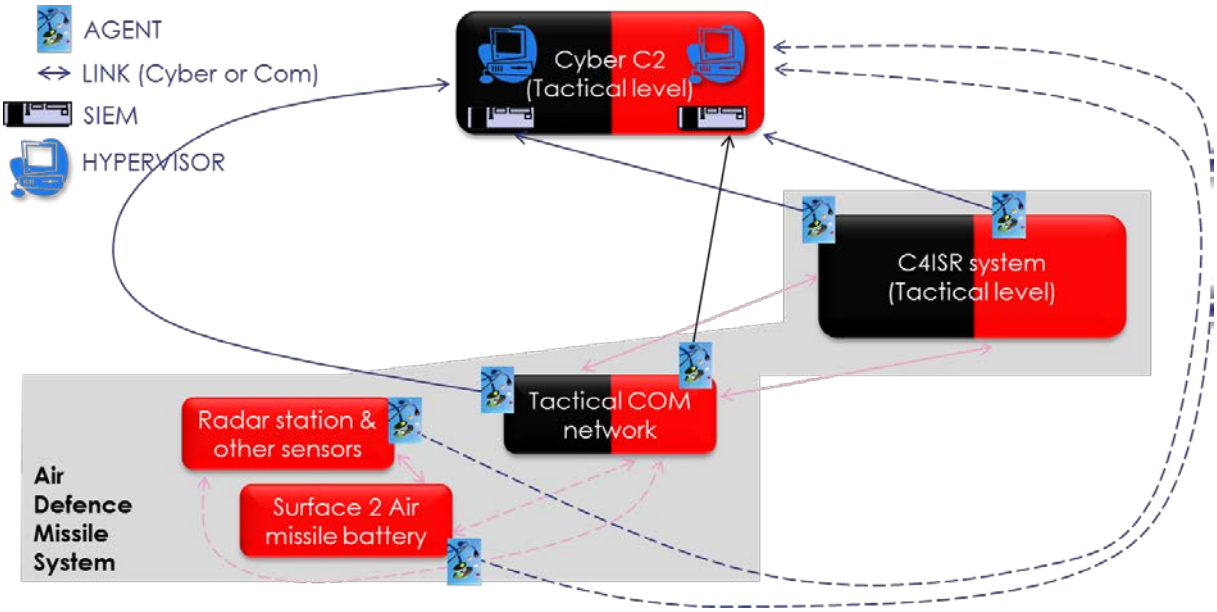

Figure 4 Example implementation of a cyber defense mechanism

Sensors are implemented within or at the periphery of effectors and across communication networks and commandment systems. Depending on circumstances they are or not permanently connected to the central Cyber-C2 (SOC). Classification levels (red or black) imply segregation.

Three broad architectural options are available for the design, implementation and operation of Autonomous Intelligent Multi Agent Systems for Cyber Defense:

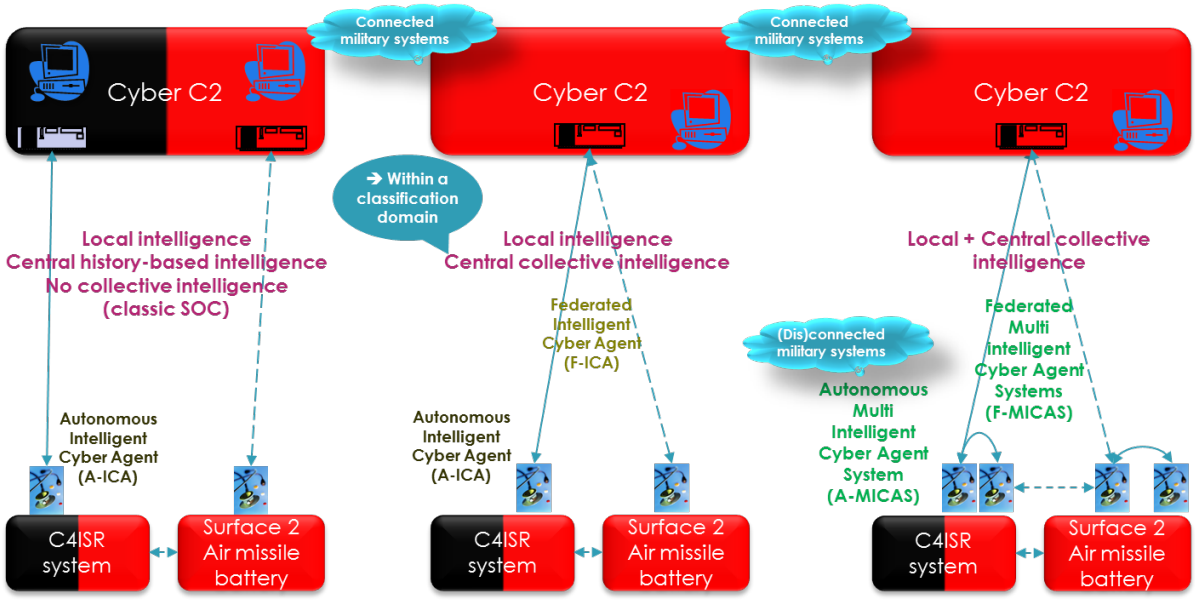

Figure 5 Architectural options for Autonomous Intelligent Multi Agent Systems for Cyber Defense

A centralized Cyber-C2 is in operation, for instance at the theater of operation level. Different levels of classification apply with each its own Cyber-C2:

- Option 1: Two levels of classification apply. An Autonomous Intelligent Cyber-Agent (A-ICA) is implemented on the restricted (black) C4ISR system and another one on the classified (red)

Surface to Air missile battery, the latter being possibly disconnected at some points in time from the Cyber-C2. In this case, no collective cyber defense intelligence is developed even by the central Cyber-C2. A central cyber-threat intelligence database feeds local A-ICAs with goals, rules and IoCs as needed. Each classification level implies that such databases be duplicated too. In this option, A-ICAs could be fairly "basic" ones to match older or current generations of military systems that cannot accept the addition of cyber defense mechanisms.

- Option 2: Only one level of classification applies in a given environment, for instance red (classified). Then, all pieces of equipment supervised by the central Cyber-C2 belong in the same classification level. One A-ICA is implemented within or at the periphery of each piece of equipment to protect, the C4ISR system and Surface to Air missile battery. The A-ICAs could develop a form of collective intelligence with the support of the central Cyber-C2. In this option too, A-ICAs could be fairly "basic" ones to match older or current generations of military systems that cannot accept the addition of cyber defense mechanisms.
- Option 3: In a similar context of a unique classification level, but with more modern and future generations of military systems that can accept embedded cyber defense mechanisms, A-ICAs would be grouped into Autonomous Multi Intelligent Cyber Agent Systems (A-MICAS), possibly federated through the central Cyber-C2 in a Federated Multi Intelligent Cyber Agent System (F-MICAS) spanning across all platforms.

Options 1 and 2 are for the short term while option 3 is a longer term option demanding that military systems can embark A-MICAS technologies. Option 3 represents therefore a target. Options 1 and 2 are milestones on the road to option 3.

LESSONS FROM THE USE CASE: IST 152's MASC ARCHITECTURE AS INTERIM SOLUTION

Cyber defense agents considered in NATO IST 152 RTG's Multi Agent System for Cyber defense (MASC, a temporary name) Reference Architecture would then be essentially of the A-ICA type in this context:

- Capable of handling fairly autonomously cyber-threats affecting the perimeter they defend, based on some local knowledge and intelligence;
- Able to cooperate to some extent with one another or with the central Cyber-C2.

The MASC Reference Architecture would contribute the cyber-defense of a military system or device through five integrated high-level functions:

- Sensing and world state identifier.
- Planning and action selector.
- Collaboration and negotiation.
- Action execution.
- Learning and knowledge improvement.

Figure 6 The MASC architecture's functions

Sensing & World state identifier: This allows a cyber-defense agent to acquire data from the environment and systems in which it operates as well as from itself in order to reach an understanding of the current state of the world and, should it detect risks in it, to trigger the Planning & Action selector high-level function. The Sensing & World state identifier high-level function includes two functions, Sensing and Word state identifier.

Planning and action selector: This allows a cyber-defense agent to elaborate one to several action proposals and to propose them to the Action selector function that decides the action or set of actions to execute in order to resolve the problematic world state pattern previously identified by the World state identifier function. The Planning and action selector high-level function includes two functions, Planning and Action selector.

Action selector: It operates on the basis of three data sources:

- Proposed response plans;
- Agent's goals;
- Execution constraints & requirements (e.g., Environment's Technical Configuration, etc.).

The proposed response plan is analyzed by the Action selector function in the light of the agent's current goals and of the execution constraints & requirements that may either be part of the world state descriptors gained through the Sensing & World state identifier high-level function or be stored in the agent's data repository and originated in the Learning & Knowledge improvement high-level function. The proposed response plan is then trimmed from whatever element does not fit the situation at hand, and augmented of prerequisite, preparatory or precautionary or post-execution recommended complementary actions. The Action selector thus produces an Executable Response Plan, and then submitted to the Action execution high-level function.

Collaboration and negotiation: This allows a cyber-defense agent 1) to exchange information (elaborated data) with other agents or with a central cyber C2, for instance when one of the agent's functions is not capable on its own to reach satisfactory conclusions or usable results, and 2) to negotiate with its partners the elaboration of a consolidated conclusion or result. The Collaboration and negotiation high-level function includes, at the present stage, one function, Collaboration and negotiation.

Action execution: This allows a cyber-defense agent to effect the Action selector function's decision about an Executable Response Plan (or the part of a global Executable Response Plan assigned to the agent), to monitor its execution and its effects, and to provide the agents with the means to adjust the execution of the plan (or possibly to dynamically adjust the plan?) when and as needed. The Action execution high-level function includes four functions, Action effector, Execution monitoring, Effects monitoring and Execution adjustment.

Learning and knowledge improvement: This allows a cyber-defense agent to use the agent's experience to improve progressively its efficiency with regards to all other functions. The Learning and knowledge improvement high-level function includes two functions, Learning and Knowledge improvement.

The overall functioning of a MASC agent is summarized in the following graph representing its generic process flow:

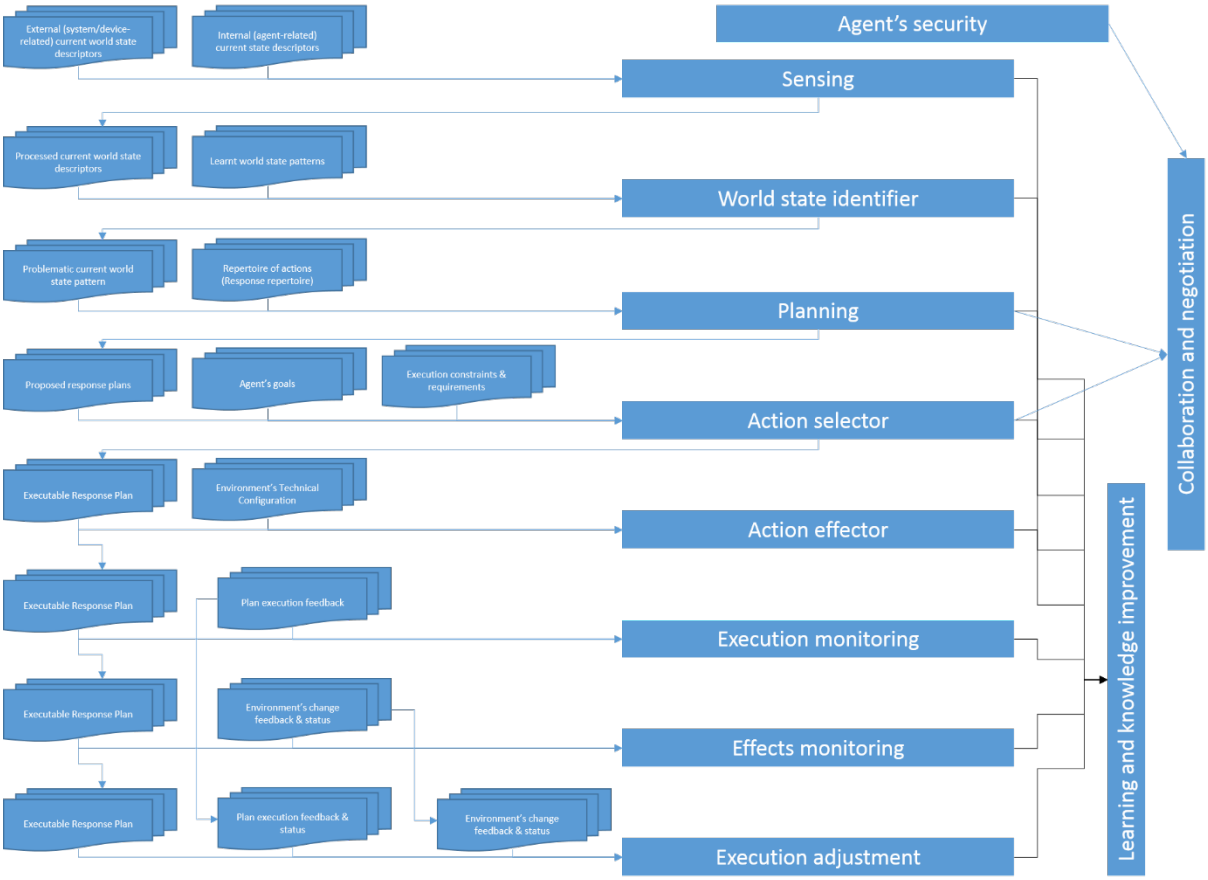

Figure 7 The generic MASC Process Flow

IN CONCLUSION

Multi Agent Systems for cyber defense are assumed to respond well to the specific constraints and requirements of the military world, including low bandwidth issues on the battlefield that may limit seriously the data transfer capacity required for cyber detection and response.

But, older generation military technologies cannot embed cyber defense mechanisms into their existing architecture. Ideal solutions, such as Autonomous Multi Intelligent Cyber Agent Systems (A-

MICAS) and Federated Multi Intelligent Cyber Agent System (F-MICAS), cannot yet be implemented. NATO IST 152's proposed MASC Reference Architecture can be an essential interim solution.

However, even this intermediate solution is no trivial endeavor. Research must still address many issues: the formal representation of agents' world of operation, from configurations of systems to attack patterns through response planning and agents' individual and collective mission goals; cyber detection and response collective intelligence and action plans methodologies; systems' observables that inform agents; agents' architectures, functionalities and capacities (e.g., memory, processing power and means); the dependable insertion of SMAs into military systems; etc. Still some time before it all happens.

REFERENCES

Bodeau, D. & Graubart, R., 2013. *Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls,* : MITRE.

Bodeau, D. J. & Graubart, R., 2011. *cyber resiliency engineering framework,* Bedford, MA: The MITRE Corporation.

CANSO, 2014. *CANSO Cyber Security and Risk Assessment Guide,* : https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf.

EMAA, 2013. *Cyberdéfense des systèmes aériens.* Paris: Etat-Major de l'Armée de l'Air.

Gowing, N. & Langdon, C., 2015. *Thinking the Unthinkable. A new imperative for leadership in the digital age.,* London: Chartered Institute of Management Accountants, available at http://www.thinkunthinkable.org/.

Jamont, J.-P., 2016. *Démarche, Modèles et outils multi-agents pour l'ingénierie des collectifs cyber-physiques.* Grenoble: Université Grenoble-Alpes, HDR, https://hal.archives-ouvertes.fr/tel-01282722.

Neumann, J. V. & Morgenstern, O., 1944. *Theory of Games and Economic Behavior.* Princeton N.J.: Princeton University Press.

NIST, 2014. *Framework for Improving Critical Infrastructure Cybersecurity,* Gaithersburg, MD: National Institute of Standards and Technology.

RT.com, 2011. *American war drones on despite virus.* [Online]
Available at: https://www.rt.com/news/virus-cyber-attack-drones-401/
[Accessed 22 08 2016].

Snyder, D., Hart, G. E., Lynch, K. F. & Drew, J. G., 2015. *Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems. Guidance for Where to Focus Mitigation Efforts,* Santa Monica, Calif: RAND Corporation, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR620/RAND_RR620.pdf.

Talukdar, S. N., 1999. Collaboration rules for autonomous software agents. *Decision Support Systems,* Volume 24, pp. 269-278.

Theron, P., 2013. ICT Resilience as dynamic process and cumulative aptitude. In: P. Theron & S. Bologna, eds. *Critical Information Infrastructure Protection and Resilience in the ICT Sector.* Hershey, PA: IGI Global.

Theron, P., 2013. ICT Resilience as dynamic process and cumulative aptitude. In: *Critical Information Infrastructure Protection and Resilience in the ICT Sector.* s.l.:IGI Global.

Théron, P., 2016. *Multi Intelligent Agent Systems and Cyber-Defence.* Paris, CYBERDEF-CYBERSEC.

US Air Force, 2008. *Air Force Cyber Command Strategic Vision,* Barksdale AFB,LA: Air Force. Air Force Cyber Command.

VENAFI, 2013. *Evolution of Cyber Attacks Infographic.* [Online]
Available at: https://www.venafi.com/blog/post/evolution-of-cyber-attacks-infographic/
[Accessed 10 July 2016].