ARL-SR-0436 ● JAN 2021

DEVCOM ARMY RESEARCH LABORATORY

Final Report of the IST-152 Group on Intelligent, Autonomous, and Trusted Agents for Cyber Defense and Resilience

by Alexander Kott

Approved for public release; distribution is unlimited.

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-SR-0436 ● JAN 2021



Final Report of the IST-152 Group on Intelligent, Autonomous, and Trusted Agents for Cyber Defense and Resilience

Alexander Kott
Office of the Director, DEVCOM Army Research Laboratory

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
January 2021	Special Report	September 2016–July 2020

4. TITLE AND SUBTITLE
Final Report of the IST-152 Group on Intelligent, Autonomous, and Trusted Agents for Cyber Defense and Resilience

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Alexander Kott

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DEVCOM Army Research Laboratory
ATTN: FCDD-RLD
Adelphi, MD 20783-1138

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-SR-0436

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
ORCID ID: Alexander Kott, 0000-0003-1147-9726

14. ABSTRACT

This document reports on the activities and outcomes of the North Atlantic Treaty Organization (NATO) Research Task Group IST-152, which was formed in 2016 and completed its work in 2020. Its topic of research was the concept of Intelligent, Autonomous, and Trusted Agents for Cyber Defense and Resilience. Twenty-one members representing 11 NATO nations actively contributed to the work of IST-152. The IST-152 Group developed a concept and a reference architecture for intelligent software agents performing active, largely autonomous cyber-defense actions on military assets. The Group published a reference architecture report where such an agent is referred to as an Autonomous Intelligent Cyber-defense Agent (AICA). In a conflict with a technically sophisticated adversary, NATO military networks will operate in a heavily contested battlefield. Enemy malware will likely infiltrate and attack friendly networks and systems. Today's reliance on human cyber defenders will be untenable. Instead, artificially intelligent agents such as AICAs will be necessary to defeat the enemy malware in an environment of potentially disrupted communications where human intervention may not be possible. In addition, the IST-152 created an Integrated Working Group for Autonomous Intelligent Cyber-defense Agents.

15. SUBJECT TERMS
intelligent agent, autonomy, cyber warfare, cyber defense, agent architecture

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Alexander Kott
Unclassified	Unclassified	Unclassified	UU	26	19b. TELEPHONE NUMBER (Include area code) (301) 394-1507

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures iv

Executive Summary v

1. Introduction and Motivation 1

2. Timeline of the IST-152 3

3. The Reference Architecture of AICA 5

3.1 A Brief Overview of the Reference Architecture 6

3.2 Potential Roadmap for AICA Development 6

3.3 Implications 7

4. The AICA Working Group 7

5. References 11

Appendix. Membership List 12

Bibliography 15

List of Symbols, Abbreviations, and Acronyms 18

Distribution List 19

List of Figures

Fig. 1 AICA reference architecture: the key components of the agent 6

Executive Summary

The North Atlantic Treaty Organization (NATO) Research Task Group IST-152 was formed in 2016 and completed its work in 2020. Its topic of research was the concept of Intelligent, Autonomous, and Trusted Agents for Cyber Defense and Resilience. The United States was appointed as the lead nation, with the Panel Mentor being Ms Cynthia Bedell (USA) and Team Leader being Alexander Kott (USA). Paul Theron (France) served as the co-leader. Twenty-one members representing 11 NATO nations actively contributed to the work of IST-152. The Activity Classification Level is UNCLASSIFIED, RELEASABLE TO THE PUBLIC.

The IST-152 Group developed a concept and a reference architecture for intelligent software agents performing active, largely autonomous cyber-defense actions on military assets. The Group published a reference architecture report where such an agent is referred to as an Autonomous Intelligent Cyber-defense Agent (AICA).

In a conflict with a technically sophisticated adversary, NATO military networks will operate in a heavily contested battlefield. Enemy malware will likely infiltrate and attack friendly networks and systems. Today's reliance on human cyber defenders will be untenable on the future battlefield. Instead, artificially intelligent agents such as AICAs will be necessary to defeat the enemy malware in an environment of potentially disrupted communications where human intervention may not be possible.

The IST-152 group identified specific capabilities of the AICA. For example, the AICA will have to be capable of autonomous planning and executing complex multi-step activities for defeating or degrading sophisticated adversary malware, while anticipating and minimizing resulting side effects. It will have to be capable of adversarial reasoning to battle against a thinking, adaptive malware. Crucially, the AICA will have to keep itself and its actions as undetectable as possible, using deceptions and camouflage.

The reference architecture identified the key functions, components, and their interactions for a potential reference architecture of such an agent, as well as a tentative roadmap toward the capabilities of the AICA.

In addition, the IST-152 created an Integrated Working Group for Autonomous Intelligent Cyber-defense Agents (AICA IWG). As of 2020, the AICA IWG was active and organized one workshop (joint with the NATO Communications and Information Agency) and an international conference AICA 2021, in March of 2021.

1. Introduction and Motivation

The North Atlantic Treaty Organization (NATO) Research Task Group IST-152 was formed in 2016 and completed its work in 2020. Its topic of research was the concept of Intelligent, Autonomous, and Trusted Agents for Cyber Defense and Resilience. The United States was appointed as the lead nation, with the Panel Mentor being Ms Cynthia Bedell (USA) and Team Leader being Alexander Kott (USA). Paul Theron (France) served as the co-leader. Twenty-one members representing 11 NATO nations actively contributed to the work of IST-152. (A complete membership list is found in the Appendix.) The Activity Classification Level was UNCLASSIFIED, RELEASABLE TO THE PUBLIC.

The IST-152 Research Task Group has developed and documented a reference architecture for an autonomous intelligent agent capable of residing on a military system, such as a combat vehicle, and performing cyber defense and mitigation against a malware that has penetrated the system under conditions when human involvement is unavailable.

Much of the Group's work was accomplished via a series of workshops and brainstorming sessions—systematic analysis of desired functions, decomposition, assessment of potential technical implementation approaches, review of current prototypes that embody similar functions, exchanges of views with industry and academia, and ongoing publications.

To focus the attention of the research group, the scope of the problem was limited. Under consideration is a single military platform, such as a vehicle, a vessel, or an unmanned aerial vehicle, with one or more computers residing on the platform, connected to sensors and actuators. Each computer contributes considerably to the operation of the platform or systems installed on the platform. One or more computers are assumed to have been compromised, where the compromise is either established as a fact or is suspected.

Due to the contested nature of the communications environment (e.g., the enemy is jamming the communications or radio silence is required to avoid detection by the enemy), communications between the vehicle and other elements of the friendly force are often limited and intermittent. At certain times and under some conditions, communications may be entirely impossible.[1]

Given the constraints on communications, conventional centralized cyber defense (i.e., an architecture where local sensors send cyber-relevant information to a central location where highly capable cyber-defense systems and human analysts detect the presence of malware and initiate corrective actions remotely) is often

infeasible.[2] It is also unrealistic to expect that the human warfighters residing on the platform (e.g., a vehicle) will have the necessary skills or time available to perform cyber-defense functions locally on the vehicle, even more so if the vehicle is unmanned.[3]

Therefore, cyber defense of such a platform, including its computing devices, will have to be performed by an intelligent, autonomous software agent.[4] The agent (or multiple agents per platform) will stealthily monitor the networks, detect the enemy agents while remaining concealed, and then destroy or degrade the enemy malware.[5] The agent will have to do so mostly autonomously, without support or guidance by a human expert.

In most discussions in this report, the agent is considered a monolithic piece of software. However, depending on the implementation, the agent's modules can be distributed over multiple processes or devices, or it could be implemented as a team of agents or subagents.

To fight the enemy malware that has infiltrated the friendly computer, the agent may have to take destructive actions, such as deleting or quarantining certain software. Such destructive actions are carefully controlled by the appropriate rules of engagement and are allowed only on the computer where the agent resides.

In most cases, the agent will not be able to stop the enemy from penetrating the platform's systems. However, it will be able to detect, analyze, and respond to a given threat. The actions of the agent, in general, cannot be guaranteed to preserve the availability or integrity of the functions and data of friendly computers. There is a risk that an agent's action will "break" the friendly computer, disable important friendly software, or corrupt or delete important data. Developers of the agent will attempt to design its actions and planning capability to minimize the risk. This risk, in a military environment, has to be balanced against the death or destruction caused by the enemy if the agent's action is not taken.

Provisions will be made to enable a remote controller—human or automated cyber command and control node—to fully observe, direct, and modify the actions of the agent, and even to update the agent's software as needed. However, it is recognized that such a remote control is often impossible due to the difficulties of communicating between the agent and the control node.[6] The agent, therefore, should be able to plan, analyze, and perform most or all of its actions autonomously.

Similarly, provisions should be made for the agent to collaborate with other agents (that reside on other computers); however, in many cases, because the communications are impaired or observed by the enemy, the agent has to eschew collaboration and operate alone.

The enemy malware—specifically, its capabilities and tactics, techniques, and procedures—evolves rapidly. Therefore, the agent will be capable of autonomous learning. In case the enemy malware knows that the agent exists and is likely to be present on the computer, the enemy malware will seek to find and destroy the agent. Therefore, the agent will possess techniques and mechanisms for maintaining a certain degree of stealth, camouflage, and concealment.[7] More generally, the agent takes measures that reduce the probability that the enemy malware will detect the agent. The agent is mindful of the need to exercise self-preservation and self-defense.

It is assumed here that the agent resides on a computer where it was originally installed by a human controller or an authorized process. We do envision a possibility that an agent may move itself (or move a replica of itself) to another computer. However, such propagation is assumed to occur only under exceptional and well-specified conditions, and takes place only within a friendly network—from one friendly computer to another friendly computer.

The rest of the report is organized as follows. Section 2 describes the work of the IST-152 as a timeline. Section 3 offers a brief overview of the first of the Group's two primary accomplishments: the Autonomous Intelligent Cyber-defense Agent (AICA) reference architecture. Section 4 describes the second of the Group's two primary accomplishments: the AICA Integrated Working Group that will continue the AICA-oriented work beyond the NATO activity.

2. Timeline of the IST-152

6–9 September 2016: First meeting of the group in Paris, France.

26 October 2016: Tele-meeting on WebEx.

26 January 2017: Tele-meeting on WebEx.

27–31 March 2017: Second meeting, Rome, Italy.

August 2017: Initial draft of Reference Architecture for Cyber Agents.

16–17 October 2017: Third meeting, Prague, Czech Republic.

18–20 October 2017: Workshop, Prague, Czech Republic.

January 2018: Proceedings of the IST-152 workshop published online http://ceur-ws.org/Vol-2057.

February 2018: Invited talk at the Workshop on Foundations of Autonomous Adaptive Cyber Systems, George Mason University, Fairfax, Virginia, USA.

March 2018: Report *Initial Reference Architecture of an Intelligent Autonomous Agent for Cyber Defense* (ARL-TR-8337) published.

26–28 March 2018: Paper presented at the 2018 Spring Symposium of AAAI, Palo Alto, California.

April 2018: IST-152 Workshop Report *Towards Intelligent Autonomous Agents for Cyber Defense* published.

May 2018: Paper presented: "Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture," Warsaw, Poland, ICMCIS.

22–25 May 2018: Fourth meeting, Warsaw, Poland.

12 October 2018: Keynote talk "Machine Learning for Autonomous Cyber Agents," CAMLIS Conference, Washington, DC.

15–19 October 2018: Fifth meeting, Lisbon, Portugal.

December 2018: Article "Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks," appeared in *The Cyber Defense Review* journal.

December 2018: Article "Features and Operation of an Autonomous Agent for Cyber Defense," appeared in *Computer Security and Information Assurance* journal (US DoD).

18–22 March 2019: Industry Workshop and Sixth Meeting at Cranfield University, Bedford, UK.

March 2019: Members of Research Task Group accept the workshop's recommendation to form an Integrated Working Group on Autonomous Intelligent Cyber-defence Agents (IWG AICA).

April 2019: Request submitted by IST-152 to IST panel to approve an extension for the purposes of creating AICA IWG.

June 2019: IST panel approves the extension.

July 2019–February 2020: Multiple discussions with various organizations to find a suitable umbrella framework for the AICA IWG.

June–August 2019: Final writing and editing of the Reference Architecture report.

September–October 2019: Final Reference Architecture report is published by the US Army Research Laboratory (ARL-SR-0421).

November 2019: Invited paper on AICA "Autonomous Intelligent Goodware Will Fight Autonomous Intelligent Malware: A Possible Future of Cyber Defense" presented at MILCOM.

December 2019: Paper "Intelligent Autonomous Things on the Battlefield" appears in *Artificial Intelligence for the Internet of Everything*, Academic Press.

11 March 2020: International teleconference to discuss the formation of the Organizing Committee for AICA IWG.

April 2020: Organizing Committee of AICA IWG begins its work.

July 2020: AICA IWG is essentially formed and begins de-facto operations.

July 2020: The following papers are published: "Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience" in *IEEE Security & Privacy*; "Reference Architecture of an Autonomous Agent for Cyber Defense of Complex Military Systems" in *Adaptive Autonomous Secure Cyber Systems*; "An Introductory Preview of Autonomous Intelligent Cyber-Defense Agent Reference Architecture, Release 2.0" in *The Journal of Defense Modeling and Simulation.*

September 2020: AICA IWG issues Call for Papers for 1st International Conference on Autonomous Intelligent Cyber-defence Agents (AICA 2021) to take place at École Militaire, Paris, France.

14 October 2020: Detailed mission statement of AICA IWG is published.

November 2020: The AICA IWG has now been officially registered in November as an "Association" under French Law.

31 November–1 December 2020: AICA IWG conducts a joint workshop with NATO's Communications and Information Agency (NCIA).

March 2021: AICA IWG conducts 1st International Conference on Autonomous Intelligent Cyber-defence Agents (AICA 2021), Paris, France.

3. The Reference Architecture of AICA

The main product developed by IST-152 was the Reference Architecture for Autonomous Intelligent Cyberdefense Agents. It was documented in a report: Kott A, Théron P, Drašar M, Dushku E, LeBlanc B, Losiewicz P, Guarino A, Mancini L, Panico A, Pihelgas M, Rzadca K. Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0. (ARL-SR-0421 and arXiv preprint arXiv:1803.10664. 2018 Mar 28.)

3.1 A Brief Overview of the Reference Architecture

Our initial exploration—reflected in this report—identified the key functions, components, and their interactions for a potential reference architecture of such an agent (Fig. 1).[8] To mention just a few examples, *Sensing and World State Identification* is the AICA high-level decision-making function that allows a cyber-defense agent to acquire data from the environment and systems in which it operates, as well as from itself, to reach an understanding of the current state of the world. *Planning and Action Selection* is the AICA high-level decision-making function that allows a cyber-defense agent to elaborate one to several action proposals (*Planning*) and propose them to the *Action Selection* function that decides the action or set of actions to execute.[9] *Learning* is the AICA high-level function that allows a cyber-defense agent to use the agent's experience to improve progressively its efficiency with regard to all other functions. For these and other high-level functions of AICA, our initial analysis suggests that the required technical approaches do not seem to be far beyond the current state of research.[7,10]

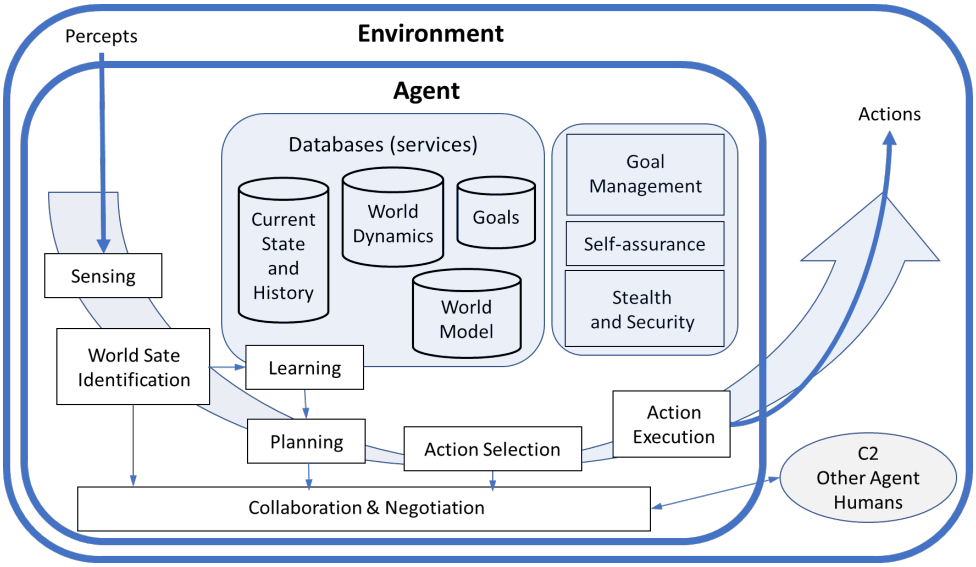


Fig. 1 AICA reference architecture: the key components of the agent

3.2 Potential Roadmap for AICA Development

Based on the analysis of the proposed AICA reference architecture and available technological foundation, we envision a roadmap toward initial yet viable capabilities. The first phase of the roadmap, which could be lasting perhaps on the order of 2 years, will include the development of knowledge-based planning of actions, the execution functionality, elements of resilient operations under attack, and adaptation of the prototype agent for execution of a small computing device. This phase would culminate in a series of Turing-like experiments that would

evaluate the capability of the agent to produce plans for remediating a compromise, as compared to experienced human cyber defenders.

The second phase, which could last about 3 years, would focus on adaptive learning, the development of a structured world model, and mechanisms for dealing with explicitly defined, multiple, and potentially conflicting goals. At this stage, the prototype agent should demonstrate the capability, in a few self-learning attempts, to return the defended system to acceptable performance after a significant change in the adversary malware behavior or techniques and procedures.

The third phase, potentially about 3–4 years, would delve into issues of multi-agent collaboration, human interactions, and ensuring both the stealth and trustworthiness of the agent. Cyber–physical challenges may need to be addressed as well. This phase would be completed when the prototype agents are able to successfully resolve a cyber compromise that could not be handled by any individual agent.

3.3 Implications

NATO cyber defense would benefit from active encouragement of AICA development efforts. Relevant research in academia and in some government and industry research organizations is growing and should be supported. It appears that academic institutions have already begun work toward AICA-like capabilities, and results are beginning to be available for transition to industry. NATO defense agencies should query the cybersecurity software vendors about availability of AICA-like products. Creating a multi-stakeholder working group engaging industry, academia, and governments could help facilitate the development of AICA technologies. NATO must not fall behind its adversaries in developing and deploying such capabilities.

4. The AICA Working Group

The second of the IST-152's two primary accomplishments was the creation of the AICA Integrated Working Group (IWG) that will continue the AICA-oriented work beyond the NATO activity.

As a follow-on to its activities, IST-152 wished to encourage the emerging interest in member nations' academia, industry and governments toward the related research and development. In particular, the participants of the Industry Workshop that took place on March 19, 2019, in Bedford, UK, expressed strong interest in forming an IWG in order for the industrial organizations to continue the work on the topic of AICA.

Therefore, a key objective of IST-152 was to encourage creation of a functioning, technically well-informed IWG that pursues several activities toward encouraging and supporting the development by industrial organizations of software based on the concept of Autonomous Agents for Cyber Defense. The ultimate goal of establishing such an IWG was to provide the NATO countries with industrial capability and actual industry-built products that constitute the next generation of cyber defense of NATO military forces.

To achieve this objective, the IST-152 performed the following activities in 2019–2020:

1) Recruited potential members of the IWG.
2) Assisted in planning and executing the inaugural meeting of the members of the IWG and provided the founding members with relevant technical insights based on the IST-152's prior work.
3) Ensured that the IWG had an adequate governance model, possibly via incorporation into an existing framework.
4) Assisted the fledgling IWG with identifying the foci of its technical efforts.

By October 2020, the AICA IWG was essentially formed and operating. Members of the IWG were recruited partly from the attendees of the Industry Workshop that took place on March 19, 2019, in Bedford, UK, as well as through other connections. The Working Group became a multi-stakeholder group (IWG) that includes not only Industry, but also Academia and Government representatives.

These IWG activities may include some or all of the following:

- developing initial common concepts and vocabulary;
- identifying functional, performance, safety, and other requirements;
- identifying or developing applicable standards;
- assembling test data sets;
- benchmarking methods;
- recommending interoperability approaches;
- proposing Verification & Validation methods;
- organizing workshops and panels on related topics;
- sponsoring competitions of the AICA products.

It is anticipated that the members of the AICA IWG will prefer to focus on those outputs that benefits all members without impeding their competitive interests. Ultimately, the AICA IWG will identify the suitable activities and outputs as its membership, and their interest, evolves.

On October 14, 2020, the AICA IWG published a detailed mission statement, beginning with the following summary:

> Faced with future hugely complex networks, systems and infrastructures on one hand, and with the anticipated huge growth of safety-critical autonomous systems on the other hand, human operators will not anymore be in a position to monitor the cybersecurity of these assets and will not be able anymore to respond to cyber-attacks at their speed, scale and level of complexity.
>
> To defend such complex and autonomous future military and civil systems against cyber-attacks, we need to embark within them Autonomous Intelligent Cyber-defence Agents (AICA) that will do the job for us, at speed and scale.
>
> Autonomous Cyber Defence (ACyD) is a new field of research & technology that presents 13 challenges.
>
> Starting for NATO IST-152's seminal AICA Reference Architecture, the Autonomous Intelligent Cyber-defence Agents International Work Group (AICA IWG) intends to develop the autonomous cyber defence science that will enable the next-generation battlefield.

On November 30 and December 1, 2020, the AICA IWG in collaboration with NATO NCIA conducted the first NCIA–AICA IWG Virtual Technical Workshop. The presentations and discussions of the workshop covered the following topics: the AICA technology and overview of its research challenges; AICA Agents' reference architecture; AICA Agents' testability and at-scale simulation; implementation and integration into host systems; decision-making within AICA Agents; AICA Agents' stealth and resilience capabilities; societal aspects—doctrines and legislation.

On March 15–16, 2021, AICA IWG will conduct the 1st International Conference on Autonomous Intelligent Cyber-defence Agents (AICA 2021). The conference plans to address the following questions:

- How should AICA agents make decisions in a complex environment and what types of decisions could those be?

- What should the structure of background knowledge and knowledge bases be that are used by AICA agents for making decisions and learning?
- How will such agents work and operate when confronted with malware agents, which can themselves be also autonomous and intelligent while possibly working in swarms?
- How should agents collaborate with one another to enhance their understanding of the cyber battlefield and to share/enhance their own resilience as well as their fighting and learning capacities?
- How will AICA agents and multi-agent systems be attacked by adversaries?
- How will AICA agents anticipate, repel, and be resilient in the presence of attacks by adversaries?
- How should we make an AICA single or multi-agent system resilient to attacks that will target them?
- What are the appropriate models of trust for AICA agents?
- How will agents learn with limited memory and computing resources?
- How will agents dynamically form and engage in heterogeneous teams?
- How will AICA systems interact with humans?
- How should an underlying AICA architecture and infrastructure support the above goals?
- What are the ethical and legal rules of engagement and societal implications of AICA agents and similar but offense-oriented technologies?
- What are the possible military/intelligence applications of AICA agents?
- What are the matrices, measurements, and methods to evaluate AICA agents?

5. References

1. Kott A, Swami A, West B. The internet of battle things. Computer. 2016;49:70–75. doi: 10.1109/MC.2016.355.
2. LeBlanc B, Losiewicz P, Hourlier S. A program for effective and secure operations by autonomous agents and human operators in communications constrained tactical environments. Proceedings of the NATO IST 152 Workshop on Intelligent, Autonomous and Trusted Agents for Cyber Defense and Resilience; 2017 Oct; NATO IST-152 Workshop.
3. Kott A, Alberts DS. How do you command an army of intelligent things? Computer. 2017;50(12):96–100.
4. Guarino A. Autonomous intelligent agents in cyber offence. In: Podins K, Stinissen J, Maybaum M, editors. 5th International Conference on Cyber Conflict – Proceedings; 2013 June 4–7; IEEE.
5. Stytz MR, Lichtblau DE, Banks SB. Toward using intelligent agents to detect, assess, and counter cyber-attacks in a network-centric environment. Institute for Defense Analyses; 2005.
6. Kott A, editor. Advanced technology concepts for command and control. Xlibris Corporation; 2004.
7. Al-Shaer E, Wei J, Hamlen KW, Wang C. Towards intelligent cyber deception systems. In: Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings. Springer; 2019.
8. Theron P, Kott A, Drašar M, Rzadca K, LeBlanc B, Pihelgas M, Mancini L, Panico A. Towards an active, autonomous and intelligent cyber defense of military systems: the NATO AICA reference architecture. In: 2018 International Conference on Military Communications and Information Systems (ICMCIS); 2018 May 22. p. 1–9. IEEE.
9. Kott A, Ground L, Budd R, Rebbapragada L, Langston J. Toward practical knowledge-based tools for battle planning and scheduling. In: AAAI/IAAI; 2002 Jul 28. p. 894–899.
10. De Gaspari F, Jajodia S, Mancini LV, Panico A. AHEAD: a new architecture for active defense. In: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig); 2016.

Appendix. Membership List

Member	Organization	Country	Email Address
Alexander Kott	US Army DEVCOM Army Research Laboratory	United States	alexander.kott1.civ@mail.mil
Paul Théron	Thales Group	France	patheron@wanadoo.fr
Luigi V Mancini	Sapienza Università di Roma	Italy	mancini@di.uniroma1.it
Edlira Dushku	Sapienza Università di Roma	Italy	dushku@di.uniroma1.it
Agostino Panico	Sapienza Università di Roma	Italy	panico@di.uniroma1.it
Martin Drašar	Masaryk University, Brno	Czech Republic	drasar@ics.muni.cz
Benoît LeBlanc	Ecole Nationale Supérieure de Cognitique	France	benoit.leblanc@ensc.fr
Paul Losiewicz	Cybersecurity and Information Systems IAC	United States	plosiewicz@quanterion.com
Alessandro Guarino	StAG Srl	Italy	a.guarino@studioag.eu
Mauno Pihelgas	NATO Cooperative Cyber-defense Centre of Excellence	Estonia	mauno.pihelgas@ccdcoe.org
Krzysztof Rzadca	Institute of Informatics, University of Warsaw	Poland	krzadca@mimuw.edu.pl
Fabio De Gaspari	Sapienza University	Italy	degaspari@di.uniroma1.it
Mauro Conti	University of Padua	Italy	conti@math.unipd.it
Nikolai Stoianov	Defense Institute	Bulgaria	n.stoianov@di.mod.bg
Michal Pechoucek	Czech Technical University	Czech Republic	Michal.pechoucek@agents.fel.cvut.cz
Pavel Celeda	Masaryk University	Czech Republic	celeda@ics.muni.cz
Nazife Baykal	Middle East Technical University	Turkey	baykal@metu.edu.tr
Ehab Al-Shaer	Carnegie Mellon University	United States	ealshaer@uncc.edu

Member	Organization	Country	Email Address
Markus Kont	NATO Cooperative Cyber-defense Centre of Excellence	Estonia	markus.kont@ccdcoe.org
Hervé Le Guyader	Ecole Nationale Supérieure de Cognitique	France	hlg@ensc.fr
Guido Gluschke	Institute for Security and Safety at Brandenburg University of Applied Sciences	Germany	g.gluschke@uniss.org

These 21 members represent 11 NATO nations.

Bibliography

Al-Rubaye S, Rodriguez J, Fragonara LZ, Theron P, Tsourdos A. Unleash narrowband technologies for industrial internet of things services. IEEE Network. 2019;33(4):16–22.

Al-Shaer E, Wei J, Hamlen KW, Wang C. Towards intelligent cyber deception systems. In: Autonomous Cyber Deception (p. 21–33). Springer, Cham; 2019.

Alsmadi I. Cyber policy and strategy management. In: The NICE Cyber Security Framework (p. 181–203). Springer, Cham; 2019.

Alsmadi I, Leslie N, Kamhoua C. Towards building actionable indicators of compromise based on a collaboration model. In: Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications (Vol. 11006, p. 110061G). International Society for Optics and Photonics; May 2019.

De Gaspari F, Jajodia S, Mancini LV, Pagnotta G. Towards intelligent cyber deception systems, [book chapter]. Springer Verlag; in press.

De Lucia M, Newcomb A, Kott A. Features and operation of an autonomous agent for cyber defense. Journal of Cyber Security and Information Systems. 2019 April;7(1).

El Namaki MSS. How companies are applying AI to the business strategy formulation. The Conversation. 2016.

Kott A. Ground warfare in 2050: How it might look. US Army Research Laboratory; 2018 August. Report No.: ARL-TN-0901.

Kott A. Intelligent autonomous agents are key to cyber defense of the future Army Networks. The Cyber Defense Review. 2018;3(3):57–70.

Kott A. Challenges and characteristics of intelligent autonomy for internet of battle things in highly adversarial environments. 2018. arXiv preprint arXiv:1803.11256.

Kott A, Rodosek GD. NATO IST-153/RWS-21 workshop on cyber resilience 2017. Proceedings of the NATO IST-153/RWS-21 Workshop on Cyber Resilience (IST-153 2017); 2017 Oct 23–25. http://ceur-ws.org/Vol-2040/

Kott A, Stump E. Intelligent autonomous things on the battlefield. In: Artificial Intelligence for the Internet of Everything (p. 47–65). Academic Press; 2019.

Kott A, Theron P. Doers, not watchers: Intelligent autonomous agents are a path to cyber resilience. IEEE Security & Privacy. 2020;18(3):62–66.

Kott A, Blakely B, Henshel D, Wehner G, Rowell J, Evans N, Muñoz-González L, Leslie N, French DW, Woodard D, Krutilla K. Approaches to enhancing cyber resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153; 2018. arXiv preprint arXiv:1804.07651.

Kott A, Mancini LV, Théron P, Drašar M, Dushku E, Günther H, Kont M, LeBlanc B, Panico A, Pihelgas M, Rzadca K. Initial reference architecture of an intelligent autonomous agent for cyber defense. US Army Research Laboratory: 2018. Report No.: ARL-TR-8337. arXiv preprint arXiv:1803.10664.

Kott A, Théron P, Drašar M, Dushku E, LeBlanc B, Losiewicz P, Guarino A, Mancini L, Panico A, Pihelgas M, Rzadca, K. Autonomous intelligent cyber-defense agent (AICA) reference architecture. Release 2.0. 2018 Mar 28. arXiv preprint arXiv:1803.10664.

Kott A, Thomas R, Drašar M, Kont M, Poylisher A, Blakely B, Theron P, Evans N, Leslie N, Singh R, Rigaki M. Toward intelligent autonomous agents for cyber defense: Report of the 2017 workshop by the North Atlantic Treaty Organization (NATO) Research Group IST-152-RTG; 2018. arXiv preprint arXiv:1804.07646.

Kott A, Théron P, Mancini LV, Dushku E, Panico A, Drašar M, LeBlanc B, et al. An introductory preview of autonomous intelligent cyber-defense agent reference architecture, release 2.0. The Journal of Defense Modeling and Simulation. 2020;17(1):51–54.

Pechoucek E, Kott A, editors. Intelligent autonomous agents for cyber defence and resilience 2017. Proceedings of the NATO IST-152 Workshop on Intelligent Autonomous Agents for Cyber Defence and Resilience (IST-152 2017); 2017 Oct 18–20. http://ceur-ws.org/Vol-2057/.

Theron P, Kott A, Drašar M, Rzadca K, LeBlanc B, Pihelgas M, Mancini L, Panico A. Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture. In: 2018 International Conference on Military Communications and Information Systems (ICMCIS) (p. 1–9). IEEE; 2018 May.

Theron P. Through-life cyber resilience in future smart manufacturing environments. A Research Programme. Procedia Manufacturing. 2018;16:193–207.

Théron P, Kott A, Drašar M, Rzadca K, LeBlanc B, Pihelgas M, Mancini L, De Gaspari F. Reference architecture of an autonomous agent for cyber defense of complex military systems. In: Adaptive Autonomous Secure Cyber Systems, p. 1–21. Springer, Cham; 2020.

Théron P, Kott A. When autonomous intelligent goodware will fight autonomous intelligent malware: A possible future of cyber defense. In: MILCOM 2019. 2019 IEEE Military Communications Conference (MILCOM), p. 1–7. IEEE; 2019.

Yamin MM, Basel KATT. Ethical problems and legal issues in development and usage autonomous adversaries in cyber domain. 2018.

List of Symbols, Abbreviations, and Acronyms

ACyD	Autonomous Cyber Defence
AICA	Autonomous Intelligent Cyber-defense Agent
IWG	Integrated Working Group
NATO	North Atlantic Treaty Organization
NCIA	NATO's Communications and Information Agency

1 (PDF)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA
1 (PDF)	DEVCOM ARL FCDD RLD DCI TECH LIB
1 (PDF)	DEVCOM ARL FCDD RLD A KOTT