T.C.
YÜKSEKÖĞRETİM KURULU BAŞKANLIĞI
Uluslararası İlişkiler Daire Başkanlığı

Sayı : 95916564-720-E.44640
Konu : NATO IST Panel Faaliyetleri

DAĞITIM YERLERİNE

İlgi : Milli Savunma Bakanlığı'nın 31.05.2019 tarihli ve 24316220-324038 sayılı yazısı.

Milli Savunma Bakanlığı'ndan alınan ilgide kayıtlı yazıda, NATO Bilim ve Teknoloji Organizasyonu (Science and Technology Organization-STO) bünyesinde faaliyet göstermekte olan Bilgi Sistemleri Teknoloji (Information Systems Technology-IST) Paneli kapsamında 13-17 Mayıs 2019 tarihleri arasında gerçekleştirilen panel toplantısında yeni başlatılacak faaliyetlere yönelik karar alındığı bildirilmektedir.

Yazıda devamla, Ön Araştırma Timi (Exploratory Team-ET) faaliyetlerinin azami bir yıl, Araştırma Görev Grubu (Research Task Group-RTG) faaliyetlerinin azami üç yıl, diğer faaliyetlerin ise kısa süreli (bir, iki veya üç gün) faaliyetler olduğu ifade edilerek, ayrıca panel bünyesindeki faaliyetlere iştirak edilmesi, faaliyetlerden beklenen kazanımların yanı sıra ülke temsili açısından da önem arz ettiği belirtilmektedir. Dolayısıyla, faaliyetlere katılım için gerekli olan kaynağın (ulaşım, konaklama, iaşe vb.) personelin mensubu bulunduğu kurum/kuruluş veya kendisi tarafından karşılanacağı, ayrıca NATO ve ilgili Bakanlıktan herhangi bir maddi destek talep edilmeyeceğinin göz önünde bulundurulması gerektiği belirtilmektedir.

Bu kapsamda ilgi yazı ile, adı geçen faaliyetlere katılım olması durumunda Ek-3'de yer alan Personel Bilgi Formu ile Ek-4'de yer alan Personel Görevlendirme ve Taahhüt Formu'nun düzenlenerek ilgili Bakanlığın Ek-1'de bilgileri yer alan resmi görevlisi ile irtibata geçilmesinin uygun olacağı değerlendirilmektedir. Ayrıca, NATO SAS Paneli bünyesinde başlatılması önerilen faaliyetlerin listesi Ek-2'de yer almaktadır.

Konunun üniversitenizin ilgili birimlerinde duyurulması hususunda gereğini rica ederim.

Prof. Dr. Rahmi ER
Başkan Vekili

Ek :
1 - İrtibat Kişisi (1 sayfa)
2 - Başlatma Kararı Alınan Faaliyetler (21 sayfa)
3 - Personel Bilgi Formu (1 sayfa)
4 - Personel Görevlendirme ve Taahhüt Formu (1 sayfa)

Üniversiteler Mah. 1600. Cad. No:10 06539 Bilkent Ankara-Türkiye
Telefon: 0(312) 298 70 00
Faks: 0(312) 266 47 59

Bilgi için:Zeynep SELVİ
Uzman

Dağıtım:

Tüm Üniversiteler(Kep)ne
Tüm Üniversiteler(Posta)ne

Üniversiteler Mah. 1600. Cad. No:10 06539 Bilkent Ankara-Türkiye
Telefon: 0(312) 298 70 00
Faks: 0(312) 266 47 59

Bilgi için:Zeynep SELVİ
Uzman

PERSONEL GÖREVLENDİRME VE TAAHHÜT FORMU

First and Last Name :

Title or Military rank and number (if applicable):

Birth Date: Birth Place: Birth Country:

Passport (by default ID Card) Number: Valid Until:

Place of Issue, Country and Date:

Nationality: Nation Represented:

Function/Department:

Organisation:

Post Office Box **and** Street Address:

Postal Code and Town:

Country:

Phone: Fax:

2nd phone:

E-mail:

2nd E-mail :

..... numaralı ..... konulu faaliyet devam ettiği sürece katılım sağlayacağımı, toplantı sonrası en geç bir ay içinde sonuç raporunu tanzim ederek göndereceğimi ve faaliyete katılım için gerekli olan kaynağın .....(Bağlı Bulunulan Kurum yada Personelin Kendisi)..... tarafından planlanacağını, ayrıca NATO ve Millî Savunma Bakanlığından herhangi bir maddi destek talep etmeyeceğimi taahhüt ederim.

Sorumlu Araştırmacının

(İ M Z A)

(Adı Soyadı)

O N A Y
(T A R İ H)

(İ M Z A)
(Kendi Kurum Amirinin)
(Adı Soyadı)
(Unvan)

NOTLAR :

1. Formdaki bilgiler İngilizce olarak doldurulacaktır.
2. Hangi faaliyete iştirak edilecekse faaliyet numarasının ve konusunun belirtilmesi gerekmektedir.
3. Özellikle formda yer alan; doğum yeri, tarihi, pasaport bilgileri ve iletişim bilgilerinin eksiksiz ve okunaklı doldurulması önem arz etmektedir.

PERSONEL BİLGİ FORMU

1. Adı Soyadı :
2. TC. Kimlik No. :
3. Rütbe/Unvanı :
4. Görev Yeri :
5. Görev Yerine Atanma Tarihi :
6. İhtisası :
7. Aday Olunan Çalışma:
8. Aday Olunan Konu İle İlgili Millî Çalışma Konuları ve Projeleri (Biliniyorsa) :
9. Aday Olunan Çalışmaya Muhtemel Katkıları :
10. Sahip Olduğu Güvenlik Kleransı (Varsa) :
11. Adresi :
12. Elektronik Posta Adresi :
13. Telefon Numarası :
14. Faks Numarası :
15. Görevlendiren Birim :
16. Kişi Güvenlik Belgesi Tarihi :
17. Diğer Hususlar :

İrtibat Kişisi:

Milli Savunma Bakanlığı
Teknik Hizmetler Dairesi Başkanlığı
Müh.Yzb.S.Çağrı DEVECİOĞLU
suleyman.devecioglu@msb.gov.tr)

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE & TECHNOLOGY ORGANIZATION

TECHNICAL ACTIVITY PROPOSAL

Panel/Group	IST	Secure Underwater Communications for Heterogeneous Network-enabled Operations	
Reference Number	**To be filled by CSO**		
Activity Type	RTG		
Panel Approval Date **To be filled by CSO**	Board Approval Date **To be filled by CSO**	Activity Start Date *JUL 19*	Activity End Date *JUL 22 (+3 years)*

Related Activity	NATO STO CMRE Workshops on Secure Underwater Communications (2017, 2018)
Projected Meeting Location(s)	Initial Meeting at CSO (Paris)
Lead Nation	UK
Team Leader(s)	Alex Hamilton (DSTL)
Panel/Group Mentor	Simon Baker (Dstl, UK)
NATO Nations/orgs. Invited To Participate	UK, US, NLD, NOR, DEU, POR NATO STO CMRE
NATO Nations/orgs. Who Endorsed The Activity	**To be filled by CSO**
Non-NATO Nations/orgs. Invited To Participate	No
Security Classification Level of the Activity	NATO RESTRICTED
Keywords	Secure, Underwater, Communications, Submarine, AUV, Autonomy, MANET
NATO and National Resources Required	Experts in areas mentioned above, funded for preparing for and attending a recurring RTG Meeting (2-4 days), and developing secure protocols and architectures for underwater networked communications. Standard publishing support.

BACKGROUND

As underwater communications capabilities are developing across several NATO nations, it is clear that we must remain interoperable in this domain. Due to the nature of undersea operations, it is of critical importance that these communications must remain secure and assured.

Furthermore, with the advent of autonomous underwater vehicles (AUVs) that are becoming more prevalent and cost-effective, a mobile undersea network can be enabled to allow secure data transfer from one nation to another.

MILITARY RELEVANCE

The initial list of benefits that will be enabled by secure underwater communications is:

- Safer operations in the underwater domain, such as for Rapid Environmental Assessment (REA), Mine Countermeasures (MCM), Anti-Submarine Warfare (ASW) and Search and Rescue (SAR) scenarios.
- Increased resilience and assurance of underwater communication by improved security awareness (authentication, integrity protection, jamming detection) and improved security measures (counter-interception by encryption, jamming resilience, anti-jamming/spoofing/tampering/hacking measures).

SCIENTIFIC OBJECTIVE(S)

This TAP is aimed at developing security standards for Underwater Communications and Networking.

Deliverables will be a report and demonstrations on the development of secure underwater communications standards and applications to joint NATO operations.

EXPECTED ACHIEVEMENTS

The task will aim to develop common use cases, network architectures and protocols to enable the underwater connectivity in a secure way. The main development will concern the security aspects, whereas the underlying protocols should be made available by partners (open or background).

This task should be supported by conceptual studies, modelling and analysis of simulation or trial results available from the contributing nations, or open source material, on secure underwater communications.

SCIENTIFIC TOPICS TO BE COVERED

- Deciding which layers to protect
    - Only application data, or also network (topology) data, and how to do so efficiently?
- Encryption and integrity-protection algorithms
    - Which algorithms to use?
    - How large can the security overhead be underwater, and how to deal with the overhead?
- Key management
    - Using symmetric or asymmetric keys?
    - How to manage the keys, which keys to use for which purpose, and how to refresh a key?

SYNERGIES AND COMPLEMENTARIES

Several nations have complementary national S&T research in this area.

There will also be a one year NIAG study in Secure UW communications running from JUL 19, this will

inform the IST RTG.

Previously CMRE has run a UW Comms security workshop that has been very successful and the outputs of this will be rolled into this IST RTG.

Research conducted under EDA Project SALSA and RACUN will look to be exploited by all nations during this tasking; furthermore releasable efforts under the UK MAR 5EYES (SOF CD MOU) will also be exploited during this RTG.

EXPLOITATION AND IMPACT

This RTG should generate NATO standards and inform operating procedure in international operations.

It will allow safe, secure and assured operations in the undersea environment. During the course of the RTG national efforts will be shared between partner nations and this will significantly increase benefits in both S&T but also capability development; creating increased capability, more robust and secure communications, and overall creating a shared and collaborative ethos for NATO underwater C5ISR development.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE & TECHNOLOGY ORGANIZATION

TECHNICAL ACTIVITY PROPOSAL

Panel/Group	*IST*	Activity Title Interoperability for Semi-Autonomous Unmanned Ground Vehicles	
Reference Number	**To be filled by CSO**		
Activity Type	*RTG*		
Panel Approval Date **To be filled by CSO**	Board Approval Date **To be filled by CSO**	Activity Start Date *1.9.2019*	Activity End Date *31.8.2022*

Related Activity	*NAAG LCG/LE ToE UGV*
Projected Meeting Location(s)	*Initial meeting will be held at CSO or at the Norwegian Defence Research Establishment in Norway. Dates to be decided.*
Lead Nation	*NOR*
Team Leader(s)	*Chair: Kim Mathiassen, NOR, Vise chair: Frank Schneider, GER*
Panel/Group Mentor	*Michael Wunder, GER or Mariann Hauge, NOR*
NATO Nations/orgs. Invited To Participate	*NOR, GER, USA, POL, EST, FIN, BEL, ESP* *NAAG LCG/LE ToE UGV*
NATO Nations/orgs. Who Endorsed The Activity	**To be filled by CSO**
Non-NATO Nations/orgs. Invited To Participate	*PfP Nations: CHE*
Security Classification Level of the Activity	*NATO UNCLASSIFIED*
Keywords	*UGV, Military robotics, Standards, Interoperability, C2*
NATO and National Resources Required	*National resources for each participating nation:* *- Travel costs for approximately two meetings per year* *- One or more of the following for the experiment: Operator Control Unit (OCU), a UGV, or a sensor, arm or other component compliant with the selected standards, or military expertise, or testing/experiment expertise.*

BACKGROUND

Interoperability is an important topic that often is taken for granted in our daily life. You can plug a device into your computer and expect it to work and e-mail and calendars are synchronized with all your devices, all this are possible because standards for communicating between devices are used. However, this simplicity has not jet come to the military domain. Still each nation's units and information systems does not communicate with each other. Standards do exists, but are still not widely used in all fields. This group would like to increase interoperability between coalition Unmanned Ground Vehicles (UGV) and their command and control (C2) systems by using standards. The group will continue the activities of RTG-149 "Capability Concept Demonstrator for Interoperability within Unmanned Ground Systems and C2" and continue to cooperate with NAAG LCG/LE ToE UGV.

MILITARY RELEVANCE

In the future UGVs will be utilized in NATO armies, at different levels of autonomy. In order for the coalition to cooperate on the battlefield it is imperative that these unmanned units may share information and that the control of the units can be shared between nations. This interoperability must be addressed together by the nations in order to address each nation's individual needs.

SCIENTIFIC OBJECTIVE(S)

The group will investigate standards to facilitate interoperability between UGVs and their C2 systems. This includes open standards / middleware solution such as JAUS[1] and ROS[2], where the latter is the de facto standard in civilian robotics research. The investigation will also include military standards such as BML[3] and IOP[4], and relevant STANAGs.

After the standards are identified, a subset of the standards will be selected. The previous group addressed tele-operation of UGVs, while we envision this group to look at a subset of standards for manned unmanned teaming, sharing information between UGVs, vehicle leader and follower and/or waypoint navigation. After the group agrees on a subset of standards and the use case, a joint experiment will be conducted to verify that systems can communicate through the implemented standards. Each participating nation will implement the agreed subset of standards on their UGV and C2 system, and the interoperability between the systems will be validated through the experiment.

After the experiment a final report will be written. This will include an account of the work done in the group and the description of the experiment. Limitations and proposed changes or enhancements of the standards will also be reported.

EXPECTED ACHIEVEMENTS

The main achievement will be a Cooperative Demonstration of Technology (CDT) where technology for interoperability will be shown. This demonstration will show an improved interaction between coalition UGVs and their C2 system compared to the capability concept demonstrator of IST-149 and ToE UGV. More specifically this group will use standards intended for higher levels of autonomy (manned/unmanned teaming, leader/follower, waypoint navigation) than the previous group (tele-operations). Possibly extending the framework established in the previous group. The TRL level will be between 5 or 6.

SCIENTIFIC TOPICS TO BE COVERED

- Interoperability for UGVs – This is the main activity for the group, and where we expect to advance. We expect that coalition UGVs can be controlled in a unified manner, so that other nations can control one nation's UGV's. We also expect to use a higher level mission definition, so that the UGVs don't have to be tele-operations.

[1] Joint Architecture for Unmanned Systems
[2] Robotic Operating System
[3] Battlefield Management Language
[4] Interoperability Profiles

- UGV technology – The group will exchange information and knowledge on UGV technology.
- Radio communication for UGV – Radio communication is very important when controlling UGVs, and is a necessary component for controlling the UGVs. Therefore we expect that this topic have to be discussed in detail and explored by the group. This could potentially also include security, data integrity and other cyber related issues. The scope is to use relevant and available radio systems, not to develop or otherwise improve the radio systems.

SYNERGIES AND COMPLEMENTARIES

Both TARDEC (US) and Fraunhofer FKIE (GER) have been developing software for easier integration between robotics system using ROS through the IOP standard. It is likely that this software can be utilized by the group, and possible further developed by the group. It is very beneficial that the group could combine its effort in creating software for interoperability, rather than everyone developing their own solution.

All participants in the group are expected to provide one of the following for the planned experiment: Operator Control Unit (OCU), a UGV, or a sensor, arm or other component compliant with the selected standards, although this is not a requirement for joining the group. Some parties might want to join as military experts or testing/experiment experts. NOR could potentially provide test range for the experiment.

EXPLOITATION AND IMPACT

UGVs are likely to provide NATO with a different set of capabilities in the future, potentially changing how war fighting is done. This group will ease the technological integration of this technology by identifying and testing standards, so that the technological basis for interoperability is ready when the UGV technology is mature enough for operational use. It will also contribute to NATO Interoperability and Standardization activities by identifying and testing standards for UGV interoperability and possibly contribute to updated standards.

The group will be a Community of Interest for the participants, where UGV related technology will be shared. NATO S&T priorities from 2016 states *Autonomy* and *Communications & Network* as two of ten S&T areas that should be prioritized. This group contributes mostly to the first area by how unmanned and potentially autonomous system should be controlled by humans, but also to the latter as the unmanned systems potentially could create a mesh networks between the systems in order to communicate with the operators.

A Cooperative Demonstration of Technology will be made at a field trial. This will demonstrate the achievements of the group and will give experience on using the standards in real conditions.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE & TECHNOLOGY ORGANIZATION

TECHNICAL ACTIVITY PROPOSAL

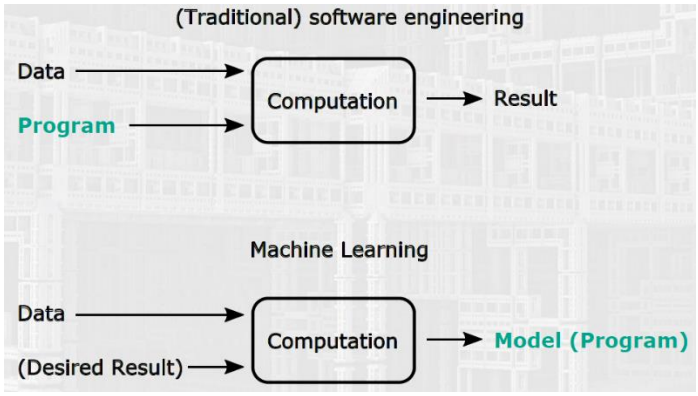
Panel/Group	*Select Panel/Group*	***Orchestration and Scalability of AI driven Systems***	
Reference Number	**To be filled by CSO**		
Activity Type	ET		
Panel Approval Date **To be filled by CSO**	Board Approval Date **To be filled by CSO**	Activity Start Date *(projected) first meeting*	Activity End Date *start date + duration*

Related Activity	*A multitude of activities with AI context is pursued, but a framework (like ITIL) is missing.*
Projected Meeting Location(s)	
Lead Nation	*DEU (proposed)*
Team Leader(s)	
Panel/Group Mentor	*Michael Wunder*
NATO Nations/orgs. Invited To Participate	*All Institutions that are involved in the production and lifecycle of IT systems*
NATO Nations/orgs. Who Endorsed The Activity	**To be filled by CSO**
Non-NATO Nations/orgs. Invited To Participate	*NATO Nations + PfP*
Security Classification Level of the Activity	*NU*
Keywords	*Software Enginering with special focus on AI systems, Trust, ML*
NATO and National Resources Required	*SME*

BACKGROUND

The elements in the life cycle of AI systems is different to ordinary SW development processes. An analogy to ITIL is not available.

One difference is the needed time for additional training phases when an AI model is extended/changed.

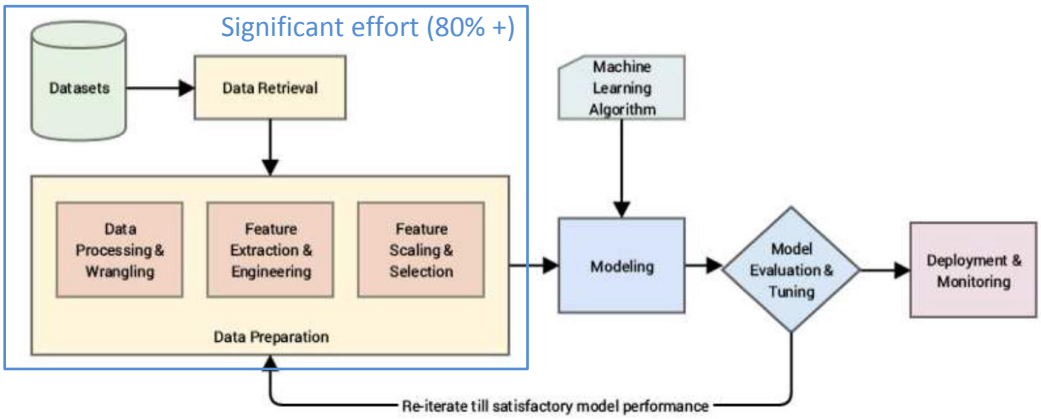


Sw developer: map a specifed logical process in Software

versus

AI model developer: generate hypothesizes, algorithmic optimizations, find proof and process training data

The purpose of the model is to allow predictions. The model is created by using AI techniques in order to find complex relations and constraints of the reality in mass data.



Source: Practical machine Learning with Python, Apress, Springer

It is not always possible to guarantee a precision of the prediction.

MILITARY RELEVANCE

See TAP on AI Infrastructure

SCIENTIFIC OBJECTIVE(S)

Invent a life cycle and SE process appropriate to AI

EXPECTED ACHIEVEMENTS

Systematize the develoment and deployment of AI systems

SCIENTIFIC TOPICS TO BE COVERED

SE …

SYNERGIES AND COMPLEMENTARIES

Higher trust in AI systems

EXPLOITATION AND IMPACT

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE & TECHNOLOGY ORGANIZATION

TECHNICAL ACTIVITY PROPOSAL

Panel/Group	IST	**Network Management & Cyber Defense (NMCD) for Federated Mission Networking (FMN)**	
Reference Number	**To be filled by CSO**		
Activity Type	RTG		
Panel Approval Date **To be filled by CSO**	Board Approval Date **To be filled by CSO**	Activity Start Date 1-1-2020	Activity End Date *tbd*
Related Activity		IST 103, FMN spirals	
Projected Meeting Location(s)		tbd	
Lead Nation		NLD (unless another Nation would like to lead)	
Team Leader(s)		tbd	
Panel/Group Mentor		COM	
NATO Nations/orgs. Invited To Participate		NLD (TNO), DEU,(Fraunhofer FKIE), FIN, GBR (DSTL), NOR (FFI), NCIA, SWE (FOI), FRA	
NATO Nations/orgs. Who Endorsed The Activity		**To be filled by CSO**	
Non-NATO Nations/orgs. Invited To Participate		EOP	
Security Classification Level of the Activity		NATO UNCLASSIFIED	
Keywords		NMCD, FMN Network Management, Cyber Defence, PCN, Data model, FMN Spiral, Interoperability,	
NATO and National Resources Required		CFBLnet Cue+ enclave	

BACKGROUND

Within IST-069-RTG the Protected Core Networking concept was developed as a means to create a non-classified transport network to be used to interconnect NATO partners within NATO missions. Using coloured clouds partners are able to form information domains on top of the transport network to exchange information among them. The IST-069-RTG produced the PCN draft Interoperabilty specification (ISpec). A number of topics that were insufficiently described in the ISpec were elaborated upon in the IST-103-RTG, among which was the definition of the Network Management and Cyber Defence capabilities of PCN. The IST-103-RTG resulted in a number of options and suggestions for the implementation of an NMCD within the PCN context.

With the implementation of Protected Core Networking in FMN Spiral 3 a need has surfaced to define a Network Management and Cyber Defence (NMCD) entity for the management and control of Protected Core Segments (PCSs) and Coloured Clouds (CCs) in the federation. It is a set of technical functions that are engineered to provide near real-time control of the network resources as well as to provide authentication and authorization of the network elements. NMCDs are federated together to provide an information domain that is dedicated to Protected Core (PCore) and CCs control and management. The NMCD entity in each separate PCS and CC needs to be able to exchange information with other NMCDs securely by using the transport service provided by the Protected Core (PCore). This information domain is implemented as Coloured Clouds associated to each and every independent PCS and CC within and connected to the PCore. These NMCD CCs have their own INFOSEC requirements, based on the security requirements of control and management information.

MILITARY RELEVANCE

FMN is the leading concept for collaboration in NATO missions. With the acceptance of PCN as network layer, the development of NMCD is paramount to ensure safe and robust information exchange under the ever growing cyber threat.

SCIENTIFIC OBJECTIVE(S)

- Specification of the NMCD functionalities for each of the upcoming FMN spirals;
- Specification of the information exchange (data model and exchange mechanism) between NMCD instances (of the mission partners);
- Implementation options for the specified NMCD functionalities;
- Interoperability tests in CWIX (for the upcoming FMN spirals).

EXPECTED ACHIEVEMENTS

At the end of the activity it will be possible to implement NMCD functionalities in such a way that the NMCD’s of different mission partners will be interoperable and able to support the PCN/FMN functionalities. This will be demonstrated in CWIX. (Is this a CDT?)

SCIENTIFIC TOPICS TO BE COVERED

- Required NMCD functionalities;
- Required information exchange for the NMCD functionalities;

- NMCD data model;
- Implementation technologies;
- Test specifications for the required NMCD functionalities;

SYNERGIES AND COMPLEMENTARIES

- IST-171-RTG FMN cloud based coalition security architecture;
- IST-142-RTG Software Defined Networking for Federated Mission Networks;

EXPLOITATION AND IMPACT

The results of this ET/RTG will be used in tests/experiments and field trials for the future FMN spirals and will in the end be used in the operational FMN. It will have most impact on Training, Material and Interoperability.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE & TECHNOLOGY ORGANIZATION

TECHNICAL ACTIVITY PROPOSAL

Panel/Group	*IST*	Activity Title *ML Ecosystem for the Rapid Research, Development, and Deployment of AI and ML Capabilities*	
Reference Number	**To be filled by CSO**		
Activity Type	*RTG*		
Panel Approval Date **To be filled by CSO**	Board Approval Date **To be filled by CSO**	Activity Start Date *June 2019*	Activity End Date *June 2022*

Related Activity	*IST-173-ST, Mission-Oriented Research for AI & Big Data for Military Decision Making; IST-178-RWS, Big Data Challenges: Situational Awareness & Decision Support*
Projected Meeting Location(s)	*TBD*
Lead Nation	*USA*
Team Leader(s)	*Dr. Lee Seversky*
Panel/Group Mentor	*Dr. Paul Antonik*
NATO Nations/orgs. Invited To Participate	*NCIA, ACT, CMRE, all NATO nations and PFP*
NATO Nations/orgs. Who Endorsed The Activity	**To be filled by CSO**
Non-NATO Nations/orgs. Invited To Participate	*PFP (SWE, FIN)*
Security Classification Level of the Activity	*NU*
Keywords	*Machine learning, artificial intelligence, computing infrastructure*
NATO and National Resources Required	*Standard CSO publication support.*

BACKGROUND

Artificial Intelligence (AI) and Machine learning (ML) are foundational to realizing future intelligent systems. AI/ML has the potential to transform how the Alliance collects, processes, shares, and analyzes diverse data types as well as how it learns, adapts to, and reasons about the environment. In just the past few years, the global pace of AI/ML advancements and application domains has undergone exponential growth – AI/ML has mastered tasks previously considered too complex for a machine - ImageNet, AlphaGo, Libratus - while doing so at a breakneck pace.

The potential for AI/ML to impact every aspect of future coalition missions is immense, spanning next generation large-scale autonomous multi-domain systems, to complex autonomous decision making. A key challenge towards realizing this potential is the ability to both rapidly leverage global AI/ML advances for military data and problem regimes as well as accelerate AI/ML research to address unique operational challenges. However, the current stovepiped approach to AI/ML is ill-equipped to take advantage of these advancements in a timely and cost efficient manner nor is it able to address the unique learning challenges that NATO must solve. As a result, the pace of development and application of AI/ML to new problems and domains across individual nations and NATO is severely limited - even in the face of large interest and need.

MILITARY RELEVANCE

The ability to develop, evaluate, and deploy ML capability rapidly and share ML capability across the alliance is critical to gaining a military advantage over global peer adversaries. The modern ML pipeline requires substantial investment in computation, data management, algorithm design and evaluation. Currently there does not exist a NATO capability for the joint development, evaluation, sharing, and reuse of ML data, algorithms, and trained models leading to individual nation duplication of MI capabilities and missed opportunities to exploit ML expertise and application subject matter experts across the alliance as well as sharing of those capabilities. The proposed ML ecosystem will enable~~d~~ NATO countries to:

a) Increase the speed of ML algorithm implementation, evaluation, and deployment through a shared NATO platform and testbed for data, algorithms, models, and evaluation metrics

b) Evaluate ML capabilities through a robust evaluation framework across NATO data, algorithms, and models to establish a repository of capability and evaluation testbed.

c) Collaborate across nations on ML R&D through an accessible ecosystem available to all NATO bodies and countries to form an Alliance community for ML R&D

SCIENTIFIC OBJECTIVE(S)

While NATO has a growing volume of valuable data obtained from Operations, exercises, and other sources, currently~~Currently~~, the Alliance lacks a common AI/ML environment to realize and capitalize on the emerging learning landscape. As a result, the Alliance is not positioned to exploit joint AI/ML advancements and overcome inherent learning challenges due to limited data access, model reuse, and the duplication of efforts across the nations and NATO bodies. Further, a common AI/ML computing and collaboration environment to foster research & development and to unite AI/ML and application domain experts is required. To address these challenges and to achieve the goal of a NATO ecosystem for bringing together data, algorithms, models, and experts, this effort can be decomposed into the following three thrusts:

- *Develop and establish a globally accessible machine learning framework to reduce the time and cost to realize SOTA ML capabilities. Through the developed framework, this activity will establish a NTO ML ecosystem that will persist and grow through contributions from all nations. Such an ecosystem will enable an accelerated means for ML research, development, and evaluation of new capabilities and has been shown to be successful in academic and commercial settings, driving contributed data repositories, collaboration, and competitions (ImageNet, FlickR, Kaggle).*

Açıklama [BA|C1]: Actually 4 bullets follow. Probably ok to remove the word "three"

- *Address the unique learning challenges inherent in NATO missions and environments. Specifically, this activity will identify real, operational learning challenges in data-efficiency, robustness, security, and interactive learning for seamless human-machine-teaming in a coalition environment.*

- *Demonstrate a core set of ML applications that have game-changing potential across the Alliance.*

- *Investigate techniques that allow the training of AI systems without releasing the training data ("bring SW to immobile data"). Make assets available without the necessity to release data.*

EXPECTED ACHIEVEMENTS

The proposed ET will explore the feasibility and scope of a NATO-wide machine learning ecosystem for the rapid research, development, and deployment of AI and ML capabilities. Specific deliverables will include:

- *An overall architecture for the ML Ecosystem, including security measures that will be required to process classified data.*
- *A 'service catalogue' defining the services that will need to be exposed by the ML Ecosystem, and an initial definition of common tools to be provided to enable AI and ML R&D and to promote interoperability between participants.*

SCIENTIFIC TOPICS TO BE COVERED

Specific technologies and problems of interest to include but are not limited to robust and data-efficient learning, interactive learning, supervised / deep learning methods, data representation challenges for ML, continuous evaluation across data, algorithms, and models, transfer learning and domain adaptation, hyper-parameter selection, and AI/ML collaborative systems and learning systems.

SYNERGIES AND COMPLEMENTARIES

Training of AI systems requires large amounts of annotated and labeled data, computing resources, and SME for the specification of use cases and evaluations. At present these resources are commonly not provided to partners within NATO preventing collaboration between interested nations and the effective exploitation of the datasets already available within NATO.

In order to bring military AI to its full potential, NATO needs an appropriate infrastructure.

AI infrastructure to be located at a new "NATO trusted Data Body" is a supporting service for the development and evaluation of military AI systems.

EXPLOITATION AND IMPACT

AI is a special focus of the IST panel. This activity will lead to better exchange of state-of-the-art knowledge on rapidly-evolving artificial intelligence and machine learning technologies.

Biçimlendirilmiş: Girinti: Sol: 0 cm

Açıklama [BA|C2]: The "NATO trusted Data Body" is not yet formally defines, but the NATO Enterprise is. Suggest rephrasing as:

"AI infrastructure accessible to bodies of the NATO Enterprise and to interested Nations is the supporting enabler required for collaborative development and evaluation of military AI systems."

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE & TECHNOLOGY ORGANIZATION

TECHNICAL ACTIVITY PROPOSAL

Panel/Group	*IST*	Blockchain Technology for Coalition Operations	
Reference Number	**To be filled by CSO**		
Activity Type	*ET*		
Panel Approval Date **To be filled by CSO**	Board Approval Date **To be filled by CSO**	Activity Start Date *March 2020*	Activity End Date *March 2023*

Related Activity	*Mention other related STO or NATO activities*
Projected Meeting Location(s)	*March 2020 CSO* *September 2020 Turkey*
Lead Nation	*Turkey*
Team Leader(s)	*Prof. Nazife Baykal*
Panel/Group Mentor	*Prof. Nazife Baykal*
NATO Nations/orgs. Invited To Participate	TBD
NATO Nations/orgs. Who Endorsed The Activity	**To be filled by CSO**
Non-NATO Nations/orgs. Invited To Participate	
Security Classification Level of the Activity	*Unclassified*
Keywords	Blockchain, Cyber security, Coalition Operations, Data Integrity, Information Security, Data Management, Resilient Information Exchange
NATO and National Resources Required	*TBD (*organization support for the meeting)

Please note that, for LTSSs, MASs and RTGs, the TAP may be expanded in Terms of Reference (ToR) and the resulting TAP should not be longer than a two-pager.

BACKGROUND

Blockchain is an emerging technology that is projected as it can offer efficient opportunities for some tasks specifically involving immutable transactions. Basically, blockchain is a shared and distributed database, which is a linked list of blocks that store transactions and digital records. What makes blockchain as a prominent technology lays down on its design features. First, it is distributed and shared by many participants. In other words, it is not controlled by a centralized authority. Being de-centralized provides no single point of failure for the network. Moreover, a blockchain network is trustless. It assumes compromises of the network by both insiders and the outsiders of the network. Second, the chain of records is immutable (i.e. append only) and tamper-resistant. As reported in the literature, the blockchain is thought to be transparently secure by relying on cryptographic data structures rather than a shared secret among the participants. This characteristic of blockchain technology provides data integrity. Lastly, every participant must agree on the records in blockchain. This introduces a common agreement on data among the participants. Based on those major characteristics, the blockchain technology has the potential to satisfy the need of reliably exchanging information over an untrusted network, where there may exist potential adversaries who try to disrupt and compromise this exchange. Furthermore, the immutable and tamper-resistant nature of the blockchain may guarantee an untampered, undistorted, and unchanged set of data records such as system and transaction logs or operational messages.

MILITARY RELEVANCE

This technology has a potential to provide integrity (in terms of preventing improper and unauthorized changes of data or resources), availability (referring the ability to use the information or resource desired), and authenticity (identification and assurance of the origin of information) required by many of the coalition operations carried out by NATO. We can think of many scenarios to utilize the blockchain technology. From the viewpoint of operations, for instance, it may provide an immutable and resilient chain of operational or tactical messages exchanged in an operation among the coalition units over the insecure channels. Or, it may be used to provide (any kind of) data integrity in regard of cyber defense. For instance, in the existence of autonomous systems and cyber physical systems, it can be employed to keep track of intact system logs for investigation in case of a cyber incident. From the viewpoint of support role, it may offer solutions to manage supply chain in an untrusted environment, where many foreign suppliers exist. Or, it may be applied to additive manufacturing, where information is threaded.
As this list of potentials of blockchain technology for coalition operations can be extended extensively, it is obvious that there is a need to research these potentials in depth to prepare NATO systems for future operations.

SCIENTIFIC OBJECTIVE(S)

The integrity of information gains more importance in case of a coalition force, where each nation has various technologies with different types and specifications of command and control systems. In this respect, the objectives of this proposal can be summarized as follows:

- Researching the pros and cons of blockchain technology from the perspective of military operations specifically from the viewpoint of coalition operations.
- Identifying the potential use-case scenarios of blockchain technology in coalition operations within NATO.
- Researching how to achieve data integrity of information exchanged among national units in a coalition force, where the underlying communication medium can be unsecure in a highly contested environment.
- Achieving an expertise in blockchain technology between NATO participants.
- Identifying the potential blockchain-based applications to partner with industry to develop these applications.
- Constructing a roadmap to employ future blockchain-based technologies and to integrate them with NATO systems and procedures.

EXPECTED ACHIEVEMENTS

- Technical report
- Conference paper
- Recommendations for future research directions
- Dissemination activity: specialist meeting

SCIENTIFIC TOPICS TO BE COVERED

Non-exhaustive list of topics to be covered:

- Blockchain technology in military operations such as naval operations
- Blockchain technology in Command and Control (C2)
- Cyber defense and cyber security (using blockchain technology in cyber security)
- Blockchain technology in autonomous systems (e.g. unmanned vehicles)
- Information security (cryptology, data integrity)
- Database systems in NATO
- Supply chain management
- Resilient communication networks

SYNERGIES AND COMPLEMENTARIES

To be completed

EXPLOITATION AND IMPACT

To be completed.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE & TECHNOLOGY ORGANIZATION

TECHNICAL ACTIVITY PROPOSAL

Panel/Group	*Select Panel/Group*	***Knowledge representation and reasoning***	
Reference Number	**To be filled by CSO**		
Activity Type	ET		
Panel Approval Date **To be filled by CSO**	Board Approval Date **To be filled by CSO**	Activity Start Date *(projected) first meeting*	Activity End Date *start date + duration*

Related Activity	*Activities related to semantic information processing and AI/ML.*
Projected Meeting Location(s)	*Video/tele-conference discussions and face-to-face meeting in Dstl, UK*
Lead Nation	*GBR (proposed)*
Team Leader(s)	*Dr. David Barber*
Panel/Group Mentor	*Bob Madahar*
NATO Nations/orgs. Invited To Participate	*All Institutions that are involved in the production and lifecycle of IT systems*
NATO Nations/orgs. Who Endorsed The Activity	**To be filled by CSO**
Non-NATO Nations/orgs. Invited To Participate	*NATO Nations + PfP*
Security Classification Level of the Activity	*NU*
Keywords	*Knowledge Management; Graph Theory, Decision Making, Semantic Information Processing*
NATO and National Resources Required	*SME*

BACKGROUND

Knowledge representation and reasoning – outline Exploratory Team (ET) proposal for NATO IST and standardisation activities

As the number of sensors, feeds and other data sources available to coalition operations increase, the focus of technology development is turning to ensuring such sources process data in-situ and provide only useful structured/pertinent observations, not least to deal with limited and intermittent network connectivity. Recently, NATO IST 144 has successfully demonstrated the potential for 'content based analytics', including the automated recognition of military hardware in video feeds and the extraction of significant entities in open reporting.

The destinations for many of those observations will be screens and dashboards that seek to provide situational awareness for human analysts. However, as the number of observations increase and the interconnections of those observations become more abstract the capacity for human analysts to make good decisions is likely to continue to be overstretched. For example, as operations look to routinely apply full spectrum effects, the interconnection of observations from the physical, social and cyber domains of operations will be increasingly important, but connections between observations in each may not be easily discernible without supporting analytical capabilities.

The integrated exploitation of observations, and therefore the representation of information and knowledge, is at the heart of concepts like "Information Advantage " and in achieving the higher level data fusion identified in the JDL Fusion Model . The real challenge now, therefore, is to be ready to integrate those observations to support situational awareness and understanding across an entire operation, enabling human/machine teams at all levels of command and across multi-national coalitions. In a coalition context this complexity also includes cultural and linguistic dimensions.

It is proposed that, in order to ensure coalition operations are able to exploit all available knowledge available to it, the following activities are established:

- *A NATO IST WG to share understanding across NATO nations on how knowledge representation and reasoning, made real through knowledge graphs can support situational awareness and understanding. This activity could include working towards a joint demonstration of capabilities against a suitable use case (building on the work of NATO IST-144).*
- *A NATO standardisation activity considering the requirements for and activities required to develop standards for the future use of knowledge graphs on coalition operations, specifically the federation of national capabilities through the use of interoperable approaches.*

MILITARY RELEVANCE

Key enabler for integration of observations to support situational awareness and understanding across an entire operation, enabling human/machine teams at all levels of command and across multi-national coalitions.

SCIENTIFIC OBJECTIVE(S)

Graph based methods, including so called "knowledge graphs" now offer the capacity to integrate multiple observations, supporting concepts like Activity Based Intelligence . However, the concept in Defence is immature and open to wide interpretation and differing approaches. Nonetheless, in other domains technology development and application continue at pace. Centres of excellence on knowledge engineering and reasoning, many with a focus on non-Defence applications, exist across NATO nations . If such approaches/technologies are to support future coalition operations joined up effort is required across a number of themes to ensure capabilities are aligned. This includes:

- *Development of domain specific ontologies*
- *Building effective architectures for event driven processing*
- *Deployment and assessment of inferencing capabilities*
- *Handling uncertainty and ambiguity in observations*
- *Information sharing and observation provenance*
- *Approaches for federated deployment and coping with scale*
- *Standards and interoperability*

EXPECTED ACHIEVEMENTS

Agreement with stakeholders and forward plan

SCIENTIFIC TOPICS TO BE COVERED

See list above

SYNERGIES AND COMPLEMENTARIES

To be completed

EXPLOITATION AND IMPACT

To be completed