TECHNICAL ACTIVITY PROPOSAL (TAP)

<table>
<tr><td>ACTIVITY REFERENCE NUMBER</td><td></td><td colspan="2" rowspan="2">Federated Interoperability of Military C2 and IoT Systems</td><td>APPROVAL
TBA</td></tr>
<tr><td>TYPE AND SERIAL NUMBER</td><td></td><td>START
01 May 2019</td></tr>
<tr><td colspan="2">LOCATION(S) AND DATES</td><td colspan="2">Locations in participating nations</td><td>END
30 Apr 2022</td></tr>
<tr><td colspan="2">COORDINATION WITH OTHER BODIES</td><td colspan="3">NCIA</td></tr>
<tr><td colspan="2">NATO CLASSIFICATION OF ACTIVITY</td><td colspan="2">U</td><td>Non-NATO Invited
YES</td></tr>
<tr><td colspan="2">PUBLICATION DATA</td><td colspan="2">TR</td><td>U</td></tr>
<tr><td>KEYWORDS</td><td colspan="4">IoT, Interoperability, Security, Federation, C2, HADR, Smart City</td></tr>
</table>

I. BACKGROUND AND JUSTIFICATION (Relevance to NATO):

The IST-147 Research Task Group (RTG) on Military Applications of the Internet of Things (IoT) explored the applicability and utility of IoT to the military domain. During the course of the last two and a half years, the activities of this group, which included experiments, demonstrations, and workshops, have demonstrated that IoT has a significant role to play in future Military Operations and Collaborative Resilience, including Humanitarian Assistance and Disaster Relief (HADR), counterterrorism, smart physiological monitoring of soldiers, and logistics and supply chain management.

Exploiting IoT capabilities and technologies has the potential to significantly increase the speed and breadth of obtaining Situation Awareness (SA) for military operations. For example, in the event of a natural disaster in a future smart city environment, being able to tap into the plethora of sensors and intelligent services within the city could enable the Military to gather SA much faster than relying solely on custom deployed sensing and information gathering. IoT is being deployed to monitor everything from weather to power grids, traffic flow, public transportation, water quality, air quality, noise pollution, medical services, and many other aspects. Being able to tap into and leverage such an information rich environment could be invaluable for future military operations.

The next challenge that naturally arises is to investigate different approaches to integrate these vast and disparate IoT systems and capabilities into existing Military Command and Control (C2) systems. Without systematic approaches to integrate these capabilities, it would be very difficult to leverage IoT capabilities in support of military operations.

Two popular approaches to enabling IoT exploitation within Military C2 systems are to either define new standards for Military IoT or to leverage the multitude of existing standards and enable federation and interoperability between these different systems. The former approach is challenging given the proliferation of existing standards and systems that are already in vogue. Defining new standards may make it more challenging to leverage existing capabilities. However, some common interfaces and data models may be necessary to enable interoperability with existing NATO and member nation C2 systems. In particular, this activity will examine Federated Mission Networking (FMN) and attempt to adopt mechanisms to allow interoperability between commercial and civilian IoT systems and FMN.

One of the results of the IST-147 activities has been to demonstrate the utility of exploiting IoT services and capabilities offered by Smart City environments, particularly for urban operations and Operations Other Than War such as HADR. However, an identified shortcoming has been the lack of standards and the challenges of discovery – to identify, connect, and leverage these Smart City IoT capabilities. Many cities and municipalities define their own standards for how this information is made available to their residents, and one off integration with each of these standards is not tractable. Hence decentralized and federated discovery capabilities need to be explored to alleviate these challenges.

Another identified challenge is security – leveraging these existing IoT capabilities implies that the military will be relying on IoT sensors, effectors, and services that owned by third parties, such as municipal governments, utility companies, or other commercial enterprises, and utilizing communications links that are similarly not secured by the military. At the very least, any military C2 system that interfaces with these types of civilian IoT capabilities must track the pedigree of any data originating or traversing these systems all the way to the military commander who might be basing his or her decisions on such data. The underlying threats of an adversary influencing or affecting this information need to be understood and mechanisms need to be developed to counter such threats. Resilient data analytics and adversary-resistant artificial intelligence methods need to be investigated in order to make sure that malicious data sources cannot unduly affect or influence decision making.

A related security challenge is that of information leakage, caused by the pervasive deployment of IoT devices within the operating environment. Leakage could occur at the RF level or at higher levels (e.g., facility level, activity level, and information level). Other risks include new attack vectors, via IoT devices, that might enable the compromise of C2 systems.

Other topics to be explored include examining existing IoT standards, as well as STANAGs, identifying those that would be worthy of either leveraging or interfacing with, developing reference architectures to enable interoperability with both military and civilian IoT, and exploring the range of possibilities of how to exercise C2 over IoT assets in a federated environment (including articulation / tasking). In the context of security, an example of such an approach could be combining civilian blockchain technologies, such as Hyperledger or Ethereum, with STANAGs 4774 and 4478 in order to provide a trusted information management approach for IoT systems used in civil-military cooperation (CIMIC) applications. A related challenge is performing collaborative data analytics in federated environments, where the individual partners might not be willing to disclose their private input data, but are interested in obtaining relevant insights from the combined data using data fusion and data analytics. An innovative technology that may enable such privacy-preserving collaborative data analytics is called Secure Multi-Party Computation, consisting of advanced (homomorphic) cryptographic techniques.

This work will build on the previous work of the IST-147 Research Task Group on Military Applications of Internet of Things.

II. OBJECTIVE(S):

1. To examine existing IoT standards, as well as existing STANAGs, architectures, and best practices to better understand how to integrate commercial and civilian IoT technologies and capabilities into Military C2 and Logistics systems, and in particular NATO's Federated Mission Networking (FMN) architecture.
2. To further define the use-cases/scenarios, interfaces, and practical usability of IoT based solutions for HADR operations in future Smart City environments and to assist in realizing Collaborative Resilience.
3. To explore the challenges of discovery of commercial IoT capabilities and services, given the relative lack of standardization.
4. To identify security challenges and develop mitigation strategies for those challenges when interfacing military C2 and civilian IoT infrastructures and when performing fusion with or otherwise relying on data coming from various sources of information.
5. To experiment and demonstrate, through proof-of-concept trials, the benefits and ability to integrate civilian IoT and military C2 systems, especially in the context of providing Collaborative Resilience.
6. To potentially engage in standardization activities in the civilian space, for example the IEEE Smart Cities initiatives.
7. To organize workshops at conferences to engage with commercial IoT activities.

III. TOPICS TO BE COVERED:

1. Scenarios that will serve as the basis for exploration and experimentation.
2. Existing standardization efforts and participation in future standardization efforts within the commercial and civilian IoT domain.

3. Examination of low-cost and COTS IoT devices for both civilian as well as military use.
4. Mechanisms necessary to interface commercial and civilian IoT with military C2 and logistics systems.
5. Federated discovery mechanisms.
6. Federated Mission Networks (FMN) and necessary interfaces / extensions to support integration of IoT with FMN.
7. Security challenges including potential threats and vulnerabilities that could be exploited by adversaries.
8. Communications challenges – both in terms of connectivity (e.g., interfacing military networks with commercial networks via gateways) and resource constraints (e.g., with tactical edge networks).

IV. DELIVERABLES:

The deliverables of the task group will be:

1. Annual demonstrations of the concepts studied and key solutions identified in a realistic military scenario. Potential venues for the demonstrations include ICMCIS and CWIX.
2. Special sessions at suitable conferences, such as the IEEE World Forum on IoT.
3. Publications of the results of the activity in journals, scientific magazines, and conferences.
4. A final report which may take the form of a book on military aspects of IoT.

V. TECHNICAL TEAM LEADER AND LEAD NATION:

Technical Team Leaders: Niranjan Suri, USA, Zbigniew Zielinski, POL
Lead nation: USA

VI. NATIONS WILLING/INVITED TO PARTICIPATE:

NATO nations: DEU, ESP, ITA, POL, NLD, NOR, USA, (awaiting confirmation from other nations)
NATO bodies: NCIA, NIAG
PfP nations: FIN, SUI

VII. NATIONAL AND/OR NATO RESOURCES NEEDED (Physical and non-physical Assets):

Host nations to provide local arrangements for meetings and workshops

VIII. CSO RESOURCES NEEDED (e.g. Consultant Funding):

Standard CSO support including ScienceConnect and WebEx or other teleconference system.
Support for open access publication of results in leading international journals or as a book