Leveraging and Fusing Civil and Military Sensors to support Disaster Relief Operations in Smart Environments

Konrad Wrona*†, Mauro Tortonesi‡, Michał Marks§, and Niranjan Suri¶‖
*NATO Communications and Information Agency, The Hague, The Netherlands
†Military University of Technology, Warsaw, Poland
‡University of Ferrara, Ferrara, Italy
§Research and Academic Computer Network, Warsaw, Poland
¶US Army Research Laboratory, Adelphi, MD USA
‖Florida Institute for Human & Machine Cognition, Pensacola, FL USA

***Abstract*—Natural disasters occur unpredictably and can range in severity from something locally manageable to large scale events that require external intervention. In particular, when large scale disasters occur, they can cause widespread damage and overwhelm the ability of local governments and authorities to respond. In such situations, Civil-Military Cooperation (CIMIC) is essential for a rapid and robust Humanitarian Assistance and Disaster Relief (HADR) operation. These type of operations bring to bear the Command and Control (C2) and Logistics capabilities of the military to rapidly deploy assets to help with the disaster relief activities. Smart Cities and Smart Environments, embedded with IoT, introduce multiple sensing modalities that typically provide wide coverage over the deployed area. Given that the military does not own or control these assets, they are sometimes referred to as gray assets, which are not as trustworthy as blue assets, owned by the military. However, leveraging these gray assets can significantly improve the ability for the military to quickly obtain Situational Awareness (SA) about the disaster and optimize the planning of rescue operations and allocation of resources to achieve the best possible effects. Fusing the information from the civilian IoT sensors with the custom military sensors could help validate and improve trust in the information from the gray assets. The focus of this paper is to further examine this challenge of achieving Civil-Military cooperation for HADR operations by leveraging and fusing information from gray and blue assets.**

***Index Terms*—Civil-military cooperation, humanitarian assistance and disaster relief, security, smart cities.**

I. Introduction

Natural disasters occur unpredictably and can range in severity from something locally manageable to large scale events that require external intervention. In particular, when large scale disasters occur, they can cause widespread damage and overwhelm the ability of local governments and authorities to respond.

In such situations, Civil-Military Cooperation (CIMIC) is essential for a rapid and robust Humanitarian Assistance and Disaster Relief (HADR) operation. These type of operations bring to bear the Command and Control (C2) and Logistics capabilities of the military to rapidly deploy assets to help with the disaster relief activities.

Increasingly, CIMIC operations will take place in Smart Environments, such as Smart Cities, which rely on the widespread deployment of Internet-of-Things (IoT) sensors and actuators and on pervasive computing solutions to enable smarter living and to assist the citizens' day-to-day activities [1]. CIMIC activities will be performed not only in support of HADR, but also in the context of defence and counter-terrorism operations.

Smart Environments could be useful for CIMIC operations. For instance, the sensor-rich environment coupled with analytic and alerting services can help identify trouble spots, suspicious behavior by people, suspicious vehicles that might contain explosives or other harmful materials, and infrastructure failures. Furthermore, archived data can be used for forensic analysis after undesirable events occur. Predictive analytics could even help identify failures or other issues ahead of time, enabling preemptive action.

However, building effective CIMIC solutions has historically been proven to be a difficult endeavor, even when little automation and technology sophistication is required. This is due to both technical (i.e. incompatible civilian and military technologies) and non-technical factors (i.e. different organizational cultures and trust relationships) [2], [3]. Although increasing use of COTS products and commercial standards within the military can reduce some technical compatibility challenges, developing CIMIC solutions for smart environments and for real-time systems integration is still a formidable organizational and engineering challenge, especially due to significant security and trust issues.

This paper investigates the challenges of achieving CIMIC for HADR operations while countering potential adversarial activities in Smart Environments. To this end, the authors leverage their experience from the NATO Science and Technology Organization (STO) IST-147 Research Task Group (RTG) on Military Applications of IoT. The paper begins with a discussion about the role of Smart Environments for HADR operations, analyzes the characteristics of Smart Environments, and then discusses the opportunities and challenges

they present. Finally, the paper proposes a roadmap towards bridging the gap between Smart Environments and CIMIC operations.

II. Disaster relief operations in smart environments

The concept of Smart Environments refers to the adoption of immersive Information and Communications Technology (ICT) solutions in our everyday lives to enable smarter living and to assist our day-to-day activities. Currently, Smart Cities represent the most important Smart Environment implementation, as they provide a new generation of real-time and time-critical, location-, social-, and context-aware services to their digital citizens, e.g., for emergency and healthcare, surveillance, entertainment, and social good. Private companies and governments at all levels are continuing the deployment of new capabilities to provide an ever increasing array of smart services to their citizens and residents [4].

Smart services implement sophisticated data analytics and information dissemination functions on top of a distributed architecture of software components. The architecture comprises of fixed sensor systems, mobile nodes nomadically roaming and interacting with one another opportunistically, edge devices located in proximity of raw data sources and information consumers, and the Cloud. To this end, smart services build on top of 3 pillars: IoT, distributed analytics, and heterogeneous communications.

IoT arguably represents the main enabling technology for smart services [5], [6]. More specifically, a capillary network of IoT sensors enables the collection of large quantities of environmental data, while at the same time making for a quickly deployable and expendable platform. The growing sophistication and the decreasing cost of technology for sensors and actuators implies that more and more of our living environment will become ”smart” [7].

In smart services, the raw data generated by IoT devices is analyzed through distributed computation solutions. In fact, Fog Computing has recently supplanted Cloud-centric approaches, allowing IT service developers and providers to allocate (a portion of the) information-processing tasks at the edge of the network [8]. Fog Computing solutions leverage a plethora of different edge devices, including IoT gateways, Cloudlets or Micro-Clouds, and Multi-Access Edge Computing to realize coarse grained but low latency data analysis and limit the amount of data flow throughout the network realm [9].

Finally, smart services implement exploit dynamic and heterogeneous communications. The emergence of heterogeneous networks in LTE/4G infrastructures [10], and in the consequent interest towards device-to-device (D2D) communications [11], is expected to intensify as 5G communications will be deployed. Also, a growing number of smart services, especially in smart grid applications, have started leveraging novel communication solutions, such as Long Range (LoRa) and Long Range Wide Area Networks (LoRaWAN) (both based on Chrip Spread Spectrum), Wireless M-Bus, Sigfox, and NarrowBand IoT (NB-IoT), designed for long range, low power, and low bit rate operations [12].

As a result, Smart Environments are characterized by a continuously and rapidly evolving software infrastructure, in which multiple smart services execute concurrently, competing for the available (and often scarce) bandwidth, computation, storage, and energy resources, and often implement different types of analytics on the same input data and need to deliver their results to different sets of users [13].

Smart services typically have different administrative domains. In fact, multiple entities own Smart City assets and services: some of them are publicly owned, but we envision that in the future many private players will operate in the Smart Environment market. Those will include platform providers that offer Cloud or Fog resources that can be used for computation and service providers that offer a wide array of smart services. Each entity is likely to adopt different access and interoperability policies for their ICT infrastructure.

In turn, smart services can be highly heterogeneous from the point of view of their access/entry point. In fact, the increasing adoption of virtualized resources and networks, propelled by the development of sophisticated network slicing solutions designed for 5G [14], allow providers to adopt any kind of isolation policy for their assets and services and to enforce access only from controlled entry points (such as a ReST API implemented in the Cloud).

Smart Environments could prove to be immensely useful during CIMIC operations such as HADR, in particular to quickly obtain SA about the affected areas, and then to monitor the conditions and the recovery process. However, their complex nature presents a wide array of challenges that need to be addressed in order to successfully leverage Smart Environment capabilities in CIMIC.

III. Data fusion in disaster relief operations

Data fusion in disaster relief is a process of correlating sensor data, with the objective of creating overall Situational Awareness (SA) about disaster environment. For example, in a smart city environment traffic camera feeds collected over time and space can be fused in order to identify the movement path of a particular object or set of objects. Multisensor data fusion [15] refers to a process where data coming from more than one type of sensors is fused. For example, information from microphones and seismic sensors can be fused in order to identify direction and type of moving objects, such as vehicles or human groups.

Data fusion has been intensively studied, in context of both military and civilian applications, resulting in development of a wide range of models and methods [16]. Several, often complementary, data fusion methodologies have been proposed, including information-based models [17], [18], activity-based models [19]–[22], and role-based models [23]. In military domain applications of data fusion have been particularly focused on development of a so-called common operating picture (COP), used to create SA of the battlespace.

The JDL data fusion model [24] was specifically proposed to support military applications. The 1998 revision divides data fusion into the following 5 levels: Level 0 Sub-object assessment; Level 1 Object assessment; Level 2 Situation assessment; Level 3 Impact assessment; and Level 4 Process refinement. An additional level, Level 5 User refinement, has been proposed in order to support trust, workload, attention, and SA of the human users [25]. The JDL data fusion model provides a robust approach to data fusion. However, its primarily target has been the recognition and identification of objects in the physical domain.

NATO Standardization Agreement (STANAG) 4162 [26] defines a standard technical characteristic of the NATO Identification System (NIS) Identification Data Combining Process (IDCP). The IDCP consists of four major sub-functions: 1) data association and track data correlation; 2) single source processing; 3) fusion; and 4) final identity category decision. The NIS IDCP accepts identification from multiple sources, associates incoming identification information to a specific track, including any existing information on that track, and converts the identification information into a form suitable for combining it in order to provide an Identity Category recommendation to the operator. In addition to representing battlefield entities, a track can be interpreted as any set of information, which is assumed to be related to the same entity. In principle, all types of identification data sensors and sources can provide input to the IDCP, and the output of the IDCP function is to be in a form suitable to meet various user applications. The operator (or so-called Identification Authority) is responsible for the final identity decision and is able at any time to manually override an identity provided from the IDCP.

Although the above mentioned data fusion models are widely used in military context they are only partially applicable to fusion of civilian and military data as encountered in disaster relief operations. In particular, although they were successfully used to fuse data of various quality and accuracy, the common assumption in the existing data fusion applications is that the data is collected only from trusted sources and any errors are mainly due to potential malfunctions or are random in nature. The trust relation is achieved via separate means and protocols, such as an appropriate sensor authentication and protection of communication channels, as well as revocation of compromised sensors. This can be technically achieved in a controlled environment operated by a single entity, however it is much more difficult in the case of data obtained from independent and uncontrolled sources.

During past CIMIC operations, the ability of leveraging technology to perform surveillance and reconnaissance has been identified as a mission-critical capability [27]. As a consequence, it is vital that in any future operation, military forces and emergency services can effectively interconnect with locally available sensing capabilities, including both civilian smart infrastructure as well as crowd-sourced information from privately owned devices. Such interconnection might not always be possible without deploying additional technical capabilities. Similarly, it might be necessary to augment the existing local sensing capability with some additional sensors and actuators. As HADR operations are typically performed in an environment that is either hostile or difficult to control, ideally any such additional capabilities would rely on inexpensive, commercially available devices that could be exposed to a significant risk of destruction or capture by hostile operatives. At the same time, a federated CIMIC SA solution needs to provide an adequate level of security and in particular ensure protection of integrity and availability as well as assessment of trustworthiness of the obtained information.

Therefore, the challenges to achieving a federated smart CIMIC environment are threefold. First, technical interoperability between devices, networks, and applications has to be achieved. The wide heterogeneity of ownership, administrative responsibility, resource isolation, and interoperability policies in Smart Environment services and assets makes the task to bring homogeneity in this picture very challenging. The idea of bringing these multiple platforms, owners, and implementations together to enable interoperabilty at the time when they are urgently required such as in HADR operations is very difficult to realize. This is particularly the case for the military, which has its own sets of tools, techniques, and oftentimes stove piped systems for ICT. Also, military ICT assets tend to remain separate for civilian ICT assets owing to security and trust issues.

Second, the solution needs to be able to operate in a degraded ICT environment, possibly without or with limited access to external power and to the Internet. Instead, the devices would need to rely to a large extent on battery power, self-charging, or opportunistic charging techniques. Communication may rely mainly on ad hoc and peer-to-peer patterns, where connection to wide area networks is provided by infrequent edge nodes. Due to this limitation, an appropriate trade-off between local and centralized data processing and aggregation has to be achieved, e.g. relying on a fog computing paradigm and appropriate delegation of the computing load to the edge nodes.

Third, the specific challenges related to security and trust management need to be effectively addressed. As this is one of the main objectives of our work, a more detailed discussion of these challenges and possible solutions is provided in Section IV.

IV. Security-specific challenges

There are several security challenges related to fusion of data obtained from grey and blue assets - as well as to performing data fusion processes and operations during disaster relief operation in general.

A. Secure handling and processing of information

At a high level, leveraging existing grey IoT capabilities implies that the military will be relying on IoT sensors, effectors, and services that are owned by third parties, such as municipal governments, utility companies, or other commercial enterprises. This data will be transmitted over networks

and links that are also not owned and controlled by the military. Traditionally, any sensor system deployed by the military has built-in mechanisms to detect and protect against tampering. Likewise, communication links are typically encrypted to prevent a variety of attacks that are possible at the network level (e.g., spoofing, man-in-the-middle, denial of service, etc.). None of these assumptions hold true for grey assets.

As discussed in Section III, during a disaster situation the available civilian information processing capability can be severely degraded. An obvious approach is to import the grey data into the military CIS and perform data aggregation and analysis there. However, the military CIS would typically operate on a confidential or secret level and therefore the import of the data needs to be performed via an appropriately configured gateway device. The gateway will be implemented either as a one-way information transmission device, called a data diode, or a restrictive two-way information mediation device, called a guard. Both types of these devices introduce limitations on protocols and data formats that can be mediated through them. In particular, the data diodes do not allow for any end-to-end communication and feedback from the receiver - the connection is terminated at the data diode and behavior of any TCP-based protocols or any other protocols requiring feedback need to be simulated. Similarly, data acquisition via a data diode can only rely on a push from the data source.

Moreover, it is of vital importance that potentially malicious or misformatted content coming from the untrusted domain not be allowed adversely affect military systems. In order to provide such protection, the gateway devices inspect the content during the mediation process and usually allow only a very limited set of data formats and protocols to crossover from the untrusted domain into the military domain. However, the implication is that these restrictions introduce additional limitations with respect to interoperability, especially when taking into account the vast and somewhat ad-hoc IoT-related protocols, technologies, and data formats used in practice.

An alternative to processing information in the military domain is offered by performing data fusion in the civilian domain, and in particular in some of the public cloud environments. These public cloud services often provide extraordinary availability and performance, including scalability and elasticity of resources, suitable for performing most complex data fusion tasks. In the disaster response situation, the role of military responders would be potentially to restore and maintain network connectivity between local assets existing in the disaster zone and the public cloud. All data aggregation and fusion could be performed in the public cloud. This removes the need for importing unclassified data obtained from the civilian sensors to classified or otherwise secured systems operated by the military. Moreover, it also potentially enables much better interoperability with the civilian assets, as many of the public cloud IoT processing systems offer built-in support for a large set of IoT protocols.

However, the challenge here is how to ensure secure processing of potentially sensitive military data in the public cloud systems, so that fusion process could be performed efficiently. In particular, confidentiality and integrity of the data obtained from the military sensors would need to be ensured, while being processed in civilian systems. There are two basic approaches to performing such secure computation in an untrusted environment.

Firstly, the computation can be performed within *secure enclaves*, which are fully separated by the trusted hardware from the other processes executed at the same platform and are accessible and administered only by the owners of the enclaves. Several recent R&D efforts within industry and academia have focused on development of such secure remote computation solutions, e.g., [28], [29]. These solution are based on specific extensions included in the modern processor platforms, such as Intel Software Guard Extensions (SGX) and AMD Secure Encrypted Virtualization (SEV).

Secondly, the computation can be securely performed on untrusted hardware, using advanced security cryptographic methods. The solutions of interest include partial and full homomorphic encryption, multi-party computation, and format/order preserving encryption [30]. However, the ability to perform more sophisticated data analytics and fusion is severely limited by the currently available cryptographic solutions. In addition, the overhead introduced by these methods vary depending on complexity of performed operations. For example, simple operations, such as search, addition, or average can be performed relatively efficiently and quickly over the encrypted data [31].

It is also possible to implement a mixed solution, where data obtained from military sensors is fused within the classified systems and only sanitized results of this partial fusion are released to civilian domain for further fusion with civilian data. However, such solution limits significantly the scope of data fusion that can be achieved and therefore the usefulness of the obtained results.

B. Trustworthy and dependable data fusion

The implementation of the fusion process in the mixed civilian military environment brings several security challenges on its own, primarily arising from limited, or unknown, trustworthiness of information obtained from the grey assets. The straightforward inclusion of such data into the fusion process could lead to data poisoning and opens up an attack vector that can be exploited by an adversary.

At the very least, any military C2 system that interfaces with the 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 overall decision making.

In most CIMIC use cases, integrity, availability, and trustworthiness of information are the most critical aspects from the perspective of enhancing SA. While availability and integrity of data are fundamental prerequisites, they are not sufficient on their own for enabling an effective fusion of the data and, consequently, providing meaningful support to the decision making process. In order to obtain a reliable and trustworthy operational picture, while relying on heterogeneous sets of data sources, operated by independent entities, it is important to be able to document data provenance. This additional information can be used in order to ensure that an operational picture is not *poisoned* by malicious or erroneous information - thus ensuring maximum use of local information sources, while minimizing the risk introduced by incorporating such external knowledge into more trusted military and government systems.

In addition, confidentiality protection might also be an important factor in some cases. This might be due to regulatory compliance requirements [32] as well as due to building trust with the civilian population or protecting identities of participants.

In CIMIC scenarios, it is often infeasible to rely on the classical public-key infrastructure (PKI) for authentication of all parties. One of the main reasons for this is that in most cases a PKI common to all participants (especially common for both the military and civilian entities) would not exist. Moreover, there might not even be a common root of trust that could be used to build such common PKI - and there might be no technical capabilities to build and operate such an infrastructure, due to challenges related to issuance of trusted public key certificates and to validation of their revocation status. Therefore, there is a need to explore alternative mechanisms for building and maintaining trust, such as distributed ledgers [33]. These alternative solutions however have to take into account operating under adversarial conditions - and need to minimize computational and communication overhead introduced into the system. This consideration means that blockchain solutions based on proof-of-work would not be suitable in most cases for use in HADR and military operations.

C. Information sharing

As disaster relief operations would usually involve a high level of civil-military cooperation, the information sharing between military and civilian responders is of paramount importance. This might include in particular the results of the data fusion process, which might be also relevant to civilian participants. However, in the option where data is ingested from the civilian domain into the military domain and data fusion takes place in the military domain, releasing fused information back to the civilian domain is non-trivial. in order to be releasable back to the civilian domain, from where some of the input data has been obtained, the resulting data has to be assessed for their releasability and properly and securely labeled as releasable information. Such machine readable labelling can ensure that the information can be automatically processed by the guard devices on the edge of military system and released to the civilian counterpartiesin a timely. Unfortunately, an integrated approach to releasability assessment and labelling of the data obtained during the various phases of the data fusion process is not widely implemented at the moment in military CIS. Although some individual building blocks, such as common values and syntax for the metadata information, as well as standardized mechanisms for trustworthy binding of this information to the data objects, have been recently developed, the process of labelling and release are still largely manual and separated from the data generation process.

D. Resilience

Equally important is the resilience of any proposed solution. While HADR scenarios do not present the same hazards of battlefield operations, they still pose significant threats at the system integrity and survivability levels. In fact, CIMIC operation might involve subsystems that have experienced significant stress and that are partially compromised or malfunctioning – especially on the civilian side.

As a result, CIS for CIMIC operations should be able to operate with components degraded. This includes an ability to effectively recover from potential security breaches and restore capabilities in a timely manner. In particular, the interconnection of military and civilian systems should not lead to significant reduction of cyber resilience within the military domain. This is also because it is not appropriate to rule out adversarial activities, given that even in HADR scenarios, adversaries may be trying to exploit the degraded capabilities of the overall system in order to exploit it for their own goals and purposes.

V. Proposed approaches to data fusion in civil-military collaboration

There are several examples of public-private collaborations involving acquisition of information from privately owned sensors for the sake of supporting emergency response and maintenance of order. For example, the Dutch *Camera in beeld* program provides Dutch police with voluntary access to over 200,000 private surveillance cameras in the Netherlands in the case of an emergency [34]. Some similar solutions, such as Amazon Ring's Neighbors and Vivint's Streety, have also been implemented in the US, and involve voluntary sharing of recordings from smart video door bells and home cameras with the local community and police [35].

Other examples of crowdsourced sensing are provided by air traffic monitoring platforms, such as FlightAware and Flightradar24 [36], and meteorological sensors, such as Netatmo [37]. Use of localized peer-to-peer overlay networks in the context of smart disaster response systems has been also investigated in [38]. One use of geo-located social media data for crowd detection has been discussed in [39].

However, all these solutions are limited in their scope, either focusing on single types of sensors (e.g. cameras, ADS-B receivers, meteorological sensors) or on a particular vendor (e.g. Ring, Vivint, Netatmo). Moreover, they are sometimes

introducing questionable security and privacy practices, thus potentially endangering the willingness of community members to voluntarily join these systems [40].

Therefore, there is a need to develop a comprehensive approach to private-public and CIMIC collaboration in the event of emergency situations in smart environments. More specifically, interoperability for smart services could be significantly facilitated by the introduction and implementation of appropriate standards at their design time – an aspect that the architects of Smart City services should carefully consider.

At the same time, smart service designers and providers should consider resilience as an important objective and plan for interoperability under disaster conditions. More specifically, they should carefully evaluate whether the advantages, in terms of security and maintainability, offered by strict access control and resource isolation policies, are offset by an easier exploitation of smart services and assets in disaster recovery operations. Perhaps an interesting tradeoff could be the implementation of a *breaking glass* policy, whose triggering enables direct access to IoT assets, to support disaster operations.

VI. Scenarios and Challenges Targeted by the NATO STO IST-147 and IST-176 RTGs

The NATO Science and Technology Organization (STO) IST-147 Research Task Group (RTG) on Military Applications of IoT explored the applicability and utility of IoT in the military domain. During its three year duration, the activities of this group, which included experiments, demonstrations, and workshops, have established that IoT has a significant role to play in future military operations and collaborative resilience, including HADR operations, counter-terrorism, smart physiological monitoring of soldiers, and logistics and supply chain management.

In particular, the group focused on the problem of exploiting IoT capabilities and technologies to significantly increase the speed and breadth of obtaining 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.

Demonstrations given by IST-147 group utilized the data obtained from both grey and blue assets. Among the problems that were identified, the most important was assessing the trustworthiness of information gathered from public/private sources like street cameras, city API sources, civilian smartphones, and meteorological sensors. There is no general solution that could have been applied in a straightforward manner. The classical security consideration to isolate systems from untrusted data was not an option in the SA scenario.

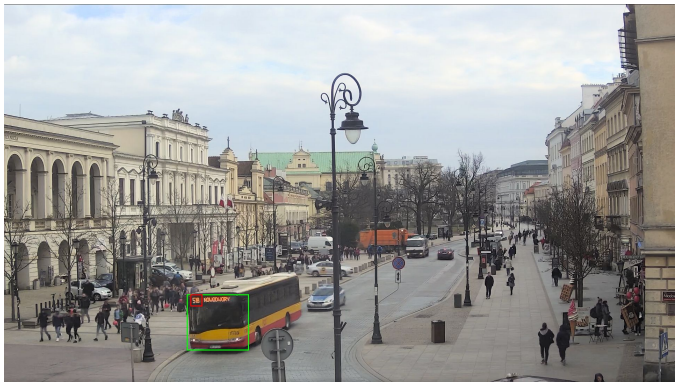

Fig. 1. Video image from street camera in Warsaw with 518 line bus annotated.

Instead, we decided to adopt a location-based cross-validation technique. For example one of the data sources that was made publicly available by the Warsaw city was the public transport information. The service gives the opportunity to get the GPS location of all the trams and buses in the city area. In conjunction with information about the GPS coordinates of street cameras, it is possible to validate the camera readings by checking if the bus or tram is visible in the particular field or not – see Figure 1. We note that this type of cross-validation technique requires time synchronization between information sources because the data aggregator receives data with different propagation delays and is thus incapable of reconstructing the originating transmission time. In the considered scenario, the video image can be gathered in real time, but the bus locations are updated every 60 seconds. As a result, in order to validate if the data sources are coherent a video image buffer must be applied. If the data received from them is consistent, grey information sources can be marked with higher trust levels; if not, the sources should be classified as untrusted or outright ignored. A similar validation scheme can be applied to verify sensor data readings coming form different service providers.

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, one promising approach would be to expand NATO's Federated Mission Networking (FMN) to

support interoperability between commercial and civilian IoT systems and FMN.

Another 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.

The group has also been examining existing IoT standards, as well as STANAGs, and 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 CIMIC applications.

Future work for CIMIC related activities will be performed in the context of the recently created IST-176 RTG on Federated Interoperability of Military C2 and IoT Systems, which will succeed the soon to be deactivated IST-147 RTG and build on its results. In particular, the focus will be on the following topics:

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 systems, and in particular NATOs Federated Mission Networking (FMN) architecture.
2) To further define the use-cases/scenarios, interfaces, and practical usability of IoT based solutions for disaster relief operations in future Smart City environments.
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 HADR and providing collaborative resilience.
6) To engage in standardization activities in the civilian space, for example with the IEEE Smart Cities initiatives.

In particular, the plan is to develop realistic CIMIC scenarios that will serve as the basis for exploration and experimentation. The results of this experimentation activities will be used to engage standardization efforts within the commercial and civilian IoT domain. A related side topic will be to examine the use of low-cost and COTS IoT devices for both civilian as well as military applications. Special effort will be dedicated to development of mechanisms necessary to interface commercial and civilian IoT with military C2 systems. These mechanisms include a federated discovery mechanism and necessary interfaces / extensions to support integration of IoT with Federated Mission Networks (FMN). The group will continue to address two key challenges in the security and communications domains. Security challenges include potential threats and vulnerabilities that could be exploited by adversaries. Communications challenges are related to both connectivity (e.g., interfacing military networks with commercial networks via gateways) and resource constraints (e.g., with tactical edge networks).

VII. Conclusions

Increasingly, disaster relief operations will take place in environments with high penetration of IoT devices. Information acquired from such Smart Environments can significantly contribute to improved situational awareness, both in terms of speed and coverage, leading to better triage and allocation of resources for the rescue and recovery operations. Smart Environments and predictive analytics could provide a range of benefits, including effective monitoring of the recovery operations, and the potential to help identify failures or other issues ahead of time, enabling preemptive action.

There are several important organizational, policy, and technical challenges that need to be overcome in order to materialize our vision of smart disaster relief operations. Technical challenges include interoperability between commercial IoT systems and military devices and networks, which tend to be stove-piped and isolated from the Internet. Another challenge is the ability for these systems to continue to operate in a degraded environment, which is often the case in the event of a large-scale disaster. However, even if the interoperability and operational challenges are solved, the critical enabler for the civil-military cooperation continues to be ability to assure the required security and trust levels. In particular, the challenges related to secure data handling and processing, dependable data fusion, sharing of data fusion results, and ensuring resilience of the complete solution need to be successfully tackled.

Developing creative and effective solutions to the above challenges requires establishment of a wider R&D collaboration. We have initiated such a collaboration within NATO STO IST-147 working group and we plan to extend it further within the follow up NATO STO IST-176 activity.

References

[1] F. Grünewald, "War in cities: Lessons learnt from the new century of urban disasters," in *War: Global Assessment, Public Attitudes and Psychosocial Effects*. Nova, 2013.

[2] M. Evans, "Future war in cities: Urbanizations challenge to strategic studies in the 21st century," *International Review of the Red Cross*, vol. 98, no. 1, pp. 37–51, 2016.

[3] A. Hoffmann, "The Urbanization of Warfare: Historical Development and Contemporary Challenges for International Humanitarian Law," *St. Antony's International Review*, vol. 12, no. 2, pp. 176–189, 2017.

[4] C. Kyriazopoulou, "Architectures and Requirements for the Development of Smart Cities : A Literature Study," in *Smartgreens 2015 and Vehits 2015*, 2015, pp. 75–103.

[5] M. Pradhan, "A survey of smart city assets for future military usage," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2018, pp. 1–6.

[6] M. Pradhan, C. Fuchs, and F. T. Johnsen, "A survey of applicability of military data model architectures for smart city data consumption and integration," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb 2018, pp. 129–134.

[7] D. Wolter and A. Kirsch, "Smart Environments: What is it and Why Should We Care?" *KI - Künstliche Intelligenz*, vol. 31, no. 3, pp. 231–237, 2017.

[8] C. Mouradian *et al.*, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

[9] M. Tortonesi *et al.*, "Taming the IoT data deluge: An innovative information-centric service model for fog computing applications," *Future Generation Computer Systems*, 2018.

[10] S. Singh, H. S. Dhillon, and J. G. Andrews, "Offloading in heterogeneous networks: Modeling, analysis, and design insights," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2484–2497, 2013.

[11] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.

[12] A. Ikpehai *et al.*, "Low-power wide area network technologies for internet-of-things: A comparative review," *IEEE Internet of Things Journal*, pp. 1–1, 2018.

[13] A. Bouguettaya *et al.*, "A service computing manifesto: The next 10 years," *Communications of the ACM*, vol. 60, no. 4, pp. 64–72, 2017.

[14] I. Afolabi *et al.*, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2429–2453, third quarter 2018.

[15] M. E. Liggins, D. L. Hall, and J. Llinas, *Multi-Sensor Data Fusion: Theory and Practice*. CRC Press LLC, 2011.

[16] D. Smith and S. Singh, "Approaches to multisensor data fusion in target tracking: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 18, no. 12, pp. 1696–1710, 2006.

[17] D. Hall and J. Llinas, "An introduction to multisensor data fusion," *Proc. IEEE*, vol. 85, no. 1, pp. 6–23, 1997.

[18] E. F. Nakamura, A. a. F. Loureiro, and A. C. Frery, "Information fusion for wireless sensor networks," *ACM Comput. Surv.*, vol. 39, no. 3, pp. 9–es, 2007.

[19] E. Shahbazian, D. Blodgett, and P. Labbé, "The extended OODA model for data fusion systems," in *Proc. 4th Int. Conf. Inf. Fusion*, 2001.

[20] M. Bedworth and J. O'Brien, "The Omnibus model: a new model of data fusion?" *Ieee Aerosp. Electron. Syst. Mag.*, vol. 15, no. 4, pp. 30–36, 2000.

[21] J. Esteban, A. Starr, R. Willetts, P. Hannah, and P. Bryanston-Cross, "A review of data fusion models and architectures: Towards engineering guidelines," *Neural Comput. Appl.*, vol. 14, no. 4, pp. 273–281, 2005.

[22] W. Elmenreich, "A review on system architectures for sensor fusion applications," in *Softw. Technol. Embed. Ubiquitous Syst.*, 2007, pp. 547–559.

[23] C. Frankel and M. Bedworth, "Control, Estimation and Abstraction in Fusion Architectures: Lessons from Human Information Processing," in *ISIF*, 2000.

[24] A. N. Steinberg and C. L. Bowman, "Revision to the JDL Data Fusion Model," in *Handb. Multisens. Data Fusion*, 2nd ed., J. Llinas, D. Hall, and M. Liggins, Eds. CRC Press LLC, 2001.

[25] E. P. Blasch and S. Plano, "JDL level 5 fusion model: user refinement issues and applications in group tracking," in *Proc. SPIE*, vol. 4729, 2002, pp. 270–279.

[26] T. Kausch and F. Opitz, "Modern Principles of Identity Fusion," in *Meet. Proc. RTO-MP-SCI-143 Des. Considerations Technol. Air Def. Syst.*, 2005.

[27] B. Alexander, "Explaining Collaboration failures in Canadas Mission in Afghanistan," *Canadian Military Journal*, vol. 14, no. 4, pp. 28–39, 2014.

[28] S. Brenner, T. Hundt, G. Mazzeo, and R. Kapitza, "Secure cloud micro services using Intel SGX," in *Proc. 17th Int. IFIP Conf. Distrib. Appl. Interoper. Syst.*, vol. 10320 LNCS, 2017, pp. 177–191.

[29] F. Kelbert, F. Gregor, R. Pires, S. Kopsell, M. Pasin, A. Havet, V. Schiavoni, P. Felber, C. Fetzer, and P. Pietzuch, "SecureCloud: Secure big data processing in untrusted clouds," in *Des. Autom. Test Eur. Conf. Exhib. (DATE), 2017*, 2017, pp. 282–285. [Online]. Available: http://ieeexplore.ieee.org/document/7926999/

[30] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, ser. CCSW '11. New York, NY, USA: ACM, 2011, pp. 113–124. [Online]. Available: http://doi.acm.org/10.1145/2046660.2046682

[31] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in *Public Key Cryptography – PKC 2010*, P. Q. Nguyen and D. Pointcheval, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 420–443.

[32] The European Parliament and the Council of the European Union, "General Data Protection Regulation," *Official Journal of the European Union*, vol. L 119, no. 2016/679, pp. 1–88, 2016.

[33] K. Wrona and M. Jarosz, "Does NATO need a blockchain?" in *MILCOM Military Communications Conference*, 2018, pp. 667–672.

[34] Politie, "Camera in Beeld," 2019. [Online]. Available: https://www.politie.nl/themas/camera-in-beeld.html

[35] B. F. Rubin, "How Ring's Neighbors app is making home security a social thing," 12 2018. [Online]. Available: https://www.cnet.com/news/how-rings-neighbors-app-is-making-home-security-a-social-thing/

[36] M. Grothaus, "How Flight Tracking Apps Work: Volunteers," 4 2015. [Online]. Available: https://www.fastcompany.com/3044490/how-flight-tracking-apps-work

[37] F. Meier *et al.*, "Crowdsourcing air temperature from citizen weather stations for urban climate research," *Urban Climate*, vol. 19, no. February, pp. 170–191, 2017.

[38] Y. Jung, "Smart Disaster Response Through Localized Short-Term Cooperation," in *Proc. of AFI 2016*, 2017, pp. 12–21.

[39] M. ben Khalifa, R. Diaz Redondo, A. Fernandez Vilas, and S. Servia Rodriguez, "Identifying urban crowds using geo-located Social media data: a Twitter experiment in New York City," *J Intell Inf Syst*, vol. 48, pp. 287–308, 2017.

[40] S. Biddle, "For owner of Amazons Ring security cameras, strangers may have been watching too," 1 2019. [Online]. Available: https://theintercept.com/2019/01/10/amazon-ring-security-camera/