Federated Information Release Module: an outline

Reinout Pieneman (TNO), Marcel van Hekken (TNO), Roy Benda (TNO), Kees van Dongen (TNO), Willem van den Bosch (TNO) & Marco Brattinga (Ordina Netherlands)

Summary

- Digital information sharing in ad hoc civil-military teams is crucial for success in current and future missions.
- This is hampered by current security policies and security mechanisms and will not be solved by NATO's Federated Mission Network (FMN) in the near future.
- TNO is working on a concept in which civil-military information sharing for adhoc teams that addresses this issue in a quick, user-friendly and technically feasible way.

Issue

The Defense organization increasingly cooperates with other nationalities, local authorities, non-governmental organizations and private parties, often ad hoc, if a crisis situation demands and for a short period. As with the military, the work of these parties is highly computerized and digitized. In practice, digital collaboration and information sharing do not match each other. The way of working together, coordinating, communicating and sharing information with unexpected, deviant and unknown parties is difficult. (Rudack, 2016) This manifests itself in different ways. For example in the mismatch between information demand and supply in the context of collaboration. (Goldenberg, 2017)

Information management in federations where parties work together, coordinate and communicate is challenging and it is difficult to manage the desired information flows. The digital collaboration channels or integrating environments for collaboration and information sharing also do not fit well and cannot be configured in a flexible way. (Soeters, 2017)

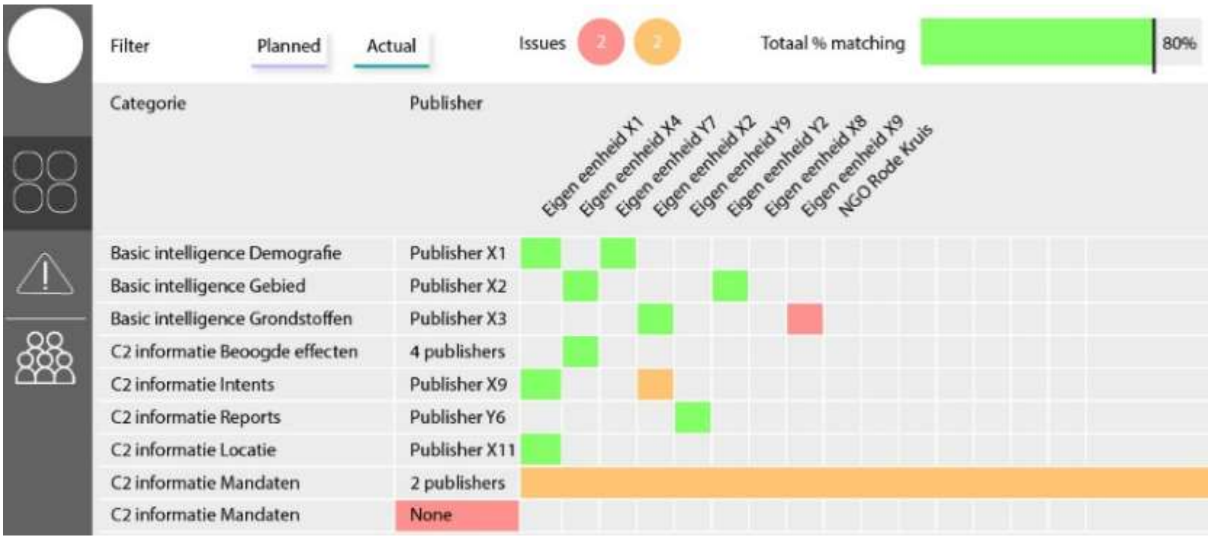
Policies and mechanisms for access to collaboration channels and information release limit information sharing. The result is that cooperation, coordination and communication is not carried out, too late, or limited or unsafe. This costs the decision-making, execution and effectiveness of missions and at the expense of the trust of partners in defense. (Goldenberg, 2017)

Concept outline

To effectively act and collaborate in ad hoc partnerships, TNO has developed the Federated Information Release Module (FIRM) concept which describes systems and processes for future federated digital collaboration. The goal of FIRM is to enable digital collaboration and fast information exchange between military parties and civil parties in ad hoc situations. More specifically, FIRM consists of three lines of development.

1. *Matching information demand and supply and managing information flows*

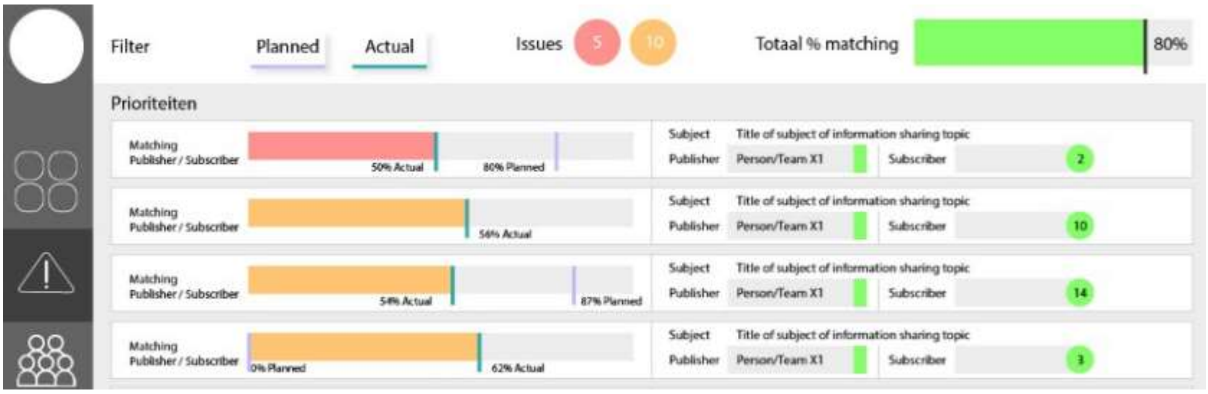
Currently, the digitization of society and the further increase in sensors implies that the amount of digital information available will significantly increase in the coming years. A challenge therefore lies in bringing together supply and demand of information and making the right information available to the user. (Suzic, 2016) With FIRM, we aim to bring together supply and demand of information via a personal information profile. The personal information profile represents the information needs and information 'offers' of a user. Based on this information, search and matching algorithms, information production and consumption from users can then be brought together. Furthermore, the personal information profiles helps to enable that information flows can be logged, monitored and, where necessary, adjusted by means of additional management tools. That way, users and information managers have insight into information flows and can optimize these where necessary. This helps to ensure that the information relevant to the user is made available automatically and in the correct form.



Filter Planned Actual Issues 2 2 Totaal % matching 80%

Categorie	Publisher	Eigen eenheid X1	Eigen eenheid X4	Eigen eenheid Y7	Eigen eenheid X2	Eigen eenheid Y9	Eigen eenheid Y2	Eigen eenheid X8	Eigen eenheid X9	NGO Rode Kruis
Basic intelligence Demografie	Publisher X1	🟩		🟩						
Basic intelligence Gebied	Publisher X2		🟩				🟩			
Basic intelligence Grondstoffen	Publisher X3				🟩				🟥	
C2 informatie Beoogde effecten	4 publishers		🟩							
C2 informatie Intents	Publisher X9	🟩			🟧					
C2 informatie Reports	Publisher Y6					🟩				
C2 informatie Locatie	Publisher X11	🟩								
C2 informatie Mandaten	2 publishers	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
C2 informatie Mandaten	None									

Fig 01: overview between produced information and consumed information with in adhoc team



Filter Planned Actual Issues 5 10 Totaal % matching 80%

Prioriteiten

Matching Publisher / Subscriber 50% Actual 80% Planned
Subject Title of subject of information sharing topic
Publisher Person/Team X1 Subscriber 2

Matching Publisher / Subscriber 56% Actual
Subject Title of subject of information sharing topic
Publisher Person/Team X1 Subscriber 10

Matching Publisher / Subscriber 54% Actual 87% Planned
Subject Title of subject of information sharing topic
Publisher Person/Team X1 Subscriber 14

Matching Publisher / Subscriber 0% Planned 62% Actual
Subject Title of subject of information sharing topic
Publisher Person/Team X1 Subscriber 3

Fig 02: detailed overview of information mis matches

2. *Setting up digital collaboration environments*

Currently, a wide variety of digital tools and collaboration environments are available. These are often not interoperable (Reliefweb, Google Drive, Titan, Extranet, Sharepoint, etc) and standard gateways, templates and processes are unavailable. (Rudac, 2016) Setting up and configuring such environments for civil-military collaboration is labor-intensive. (Suzic *et al*., 2016) FIRM therefore aims to address this issue by standardizing tooling for federative digital collaboration between civil and military parties.

Open, federated collaboration platform managed by a (set of) trusted parties, in which universal internet standards can be used to easily connect new parties, while metadata is generated so that information is easy to find. In FIRM, data and metadata are separated to enable documents to be found based on metadata labels, while data itself does not have to be shared with the platform. In addition, meta data labels help to determine the exact value of information for other users. That way, demand and supply of information can be easily matched with the help of user profiles that are built using semi-automatic metadata. (Domingo, 2015)

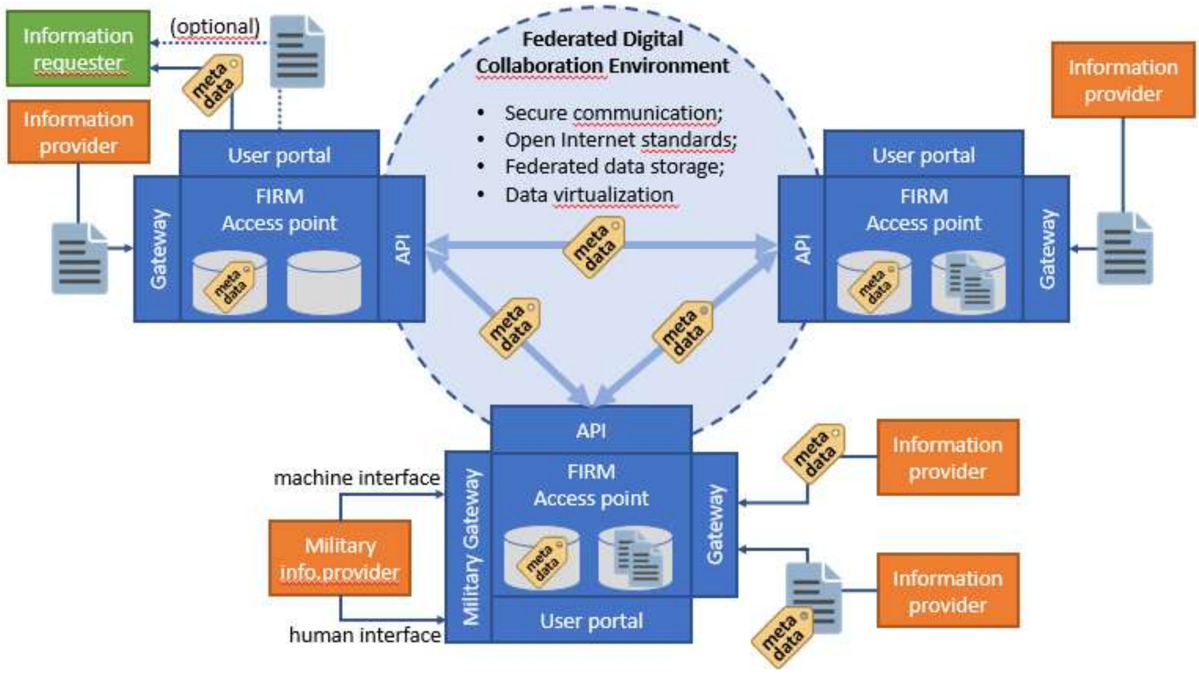
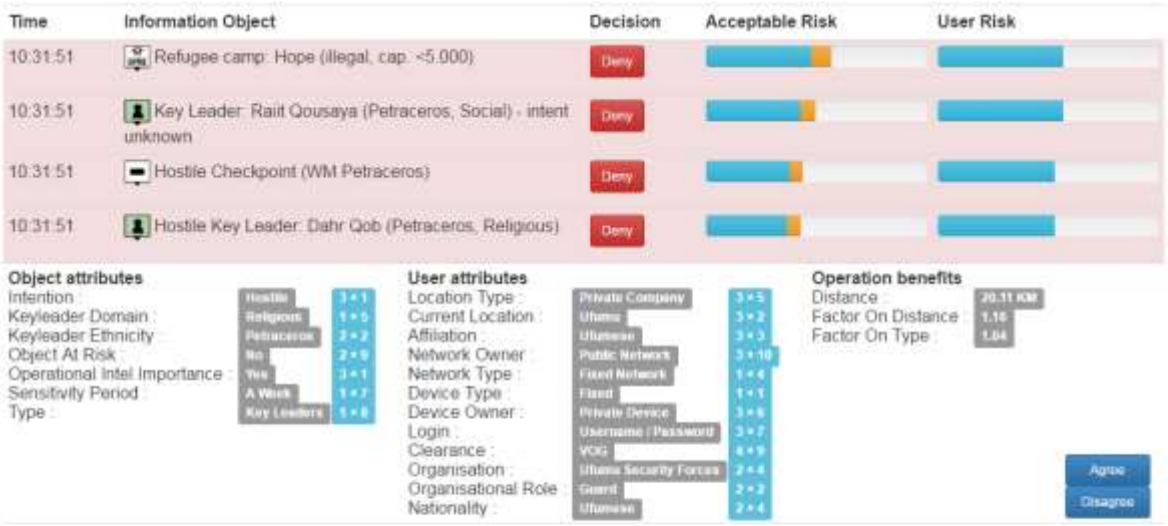


Fig 03: overview of FIRM setup

3. *Safe sharing of information*

Currently, existing security policies hamper digital sharing of classified information. To be able to share this information, the classification will need to be adjusted, or an expanded check must take place of the person with whom information is shared. As a result, the emphasis is on securing information and less on sharing information. (Dos Santos *et al*., 2016) To address this issue, FIRM aims to tackle this issue by setting up processes and systems, in which a balance is sought between the risks and the benefits of information sharing. In this risk adaptive access control (RADAC) approach, a balance is sought between the risks, but also taking account of the operational benefits of sharing information. (Atlam *et al*., 2018) By automating this metric in a way that a security officer/release officer can tailor these settings to the operational context, systems help the user to provide insight into these risks and benefits. That way, the user can share information securely digitally in a simple way. No complex procedures have to be followed.



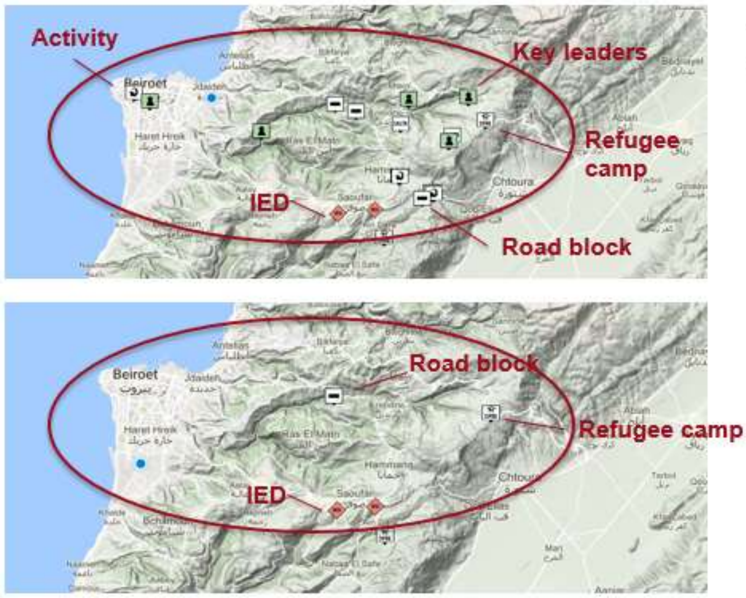
Time	Information Object	Decision	Acceptable Risk	User Risk
10:31:51	Refugee camp: Hope (illegal, cap. <5.000)	Deny		
10:31:51	Key Leader: Raiit Qousaya (Petraceros, Social) - intent unknown	Deny		
10:31:51	Hostile Checkpoint (WM Petraceros)	Deny		
10:31:51	Hostile Key Leader: Dahr Qob (Petraceros, Religious)	Deny		

Object attributes		
Intention :	Hostile	1 × 1
Keyleader Domain :	Religious	1 × 5
Keyleader Ethnicity :	Petraceros	2 × 2
Object At Risk :	No	2 × 9
Operational Intel Importance :	Yes	3 × 1
Sensitivity Period :	A Week	1 × 7
Type :	Key Leaders	1 × 8

User attributes		
Location Type :	Private Company	3 × 5
Current Location :	Uhuru	3 × 2
Affiliation :	Uhunese	3 × 3
Network Owner :	Public Network	3 × 10
Network Type :	Fixed Network	1 × 4
Device Type :	Fixed	1 × 1
Device Owner :	Private Device	3 × 6
Login :	Username / Password	3 × 7
Clearance :	VOG	4 × 9
Organisation :	Uhuru Security Forces	2 × 4
Organisational Role :	Guard	2 × 2
Nationality :	Uhunese	2 × 4

Operation benefits	
Distance :	20.11 KM
Factor On Distance :	1.16
Factor On Type :	1.04

Fig 04: Example interface for release officer



Trusted user => receives more information

Non-trusted user => receives only some basic information

Fig 05: Example interface for users with different trust levels

4. Secure networking of networks and systems

Currently, security policy does not allow the linking of the classified military networks with the mostly unclassified civilian networks. Furthermore, available gateways offer limited functionality and the release of information through such gateways is a complex and labor-intensive process. (Arnold, 2016) FIRM aims to address this issue by designing information gateways that do not give permission to share information at network level, but at application and data level. (Lubkovski *et al*., 2015) When data sets are properly labeled and indexed, a more fine grained release mechanism becomes available that can use properly secured and encrypted connections. As a result, networks and systems can be linked easily, safely and quickly. Sharing information from a classified environment becomes possible.

Conclusion

In a future mission environment in which adhoc civ-military teams need to increasingly work together, new solutions are needed to close the gap between current stovepiped digital systems. The proposed FIRM concept aims to address this issue by integrating different research strand into a single solution:

1. Matching information demand and supply
2. Setting up digital collaboration environments
3. Safe sharing of information
4. Secure networking of networks and systems

To ensure proper functioning of FIRM, a future prototype needs to be able to extract (meta) data from multiple networks and data sources. We therefore propose a more fine grained access control mechanism (RADAC) in combination with dynamic information management methods in which the information/security manager manages the FIRM gateway and can actually train the computer in release decisions. A prototype release gateway (TRL 3-4) which combines all four research strands is currently being developed.

Future research

When designing a such a prototype mechanism, we expect a number of challenges to come forward.

1. Connecting to restricted Defense networks. Development of Information Clearing House may help here. Security policies should be reviewed.
2. Labelling of data. To make this concept work data elements should be labelled with metadata. This requires discipline. This may be partly automated in the future.
3. Interoperability on application level. Civil and military partners use different applications and different standards. Aim for most used applications and standards.

The authors are open for incorporating prototype ideas and solutions into field tests.

References

Arnold, R. D. (2016). *Strategies for Transporting Data Between Classified and Unclassified Networks*. ARDEC, WSEC, RDAR-WSF-M Picatinny Arsenal United States.

Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B., & Daniel, J. (2017, June). Developing an adaptive Risk-based access control model for the Internet of Things. In *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017 IEEE International Conference on* (pp. 655-661). IEEE.

Atlam, H. F., Alenezi, A., Hussein, R. K., & Wills, G. B. (2018). Validation of an Adaptive Risk-based Access Control Model for the Internet of Things. *International Journal of Computer Network and Information Security*, *10*(1), 26.

Bellavista, P., & Montanari, R. (2017). Context Awareness for Adaptive Access Control Management in IoT Environments. *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications*, 157-178.

Bloebaum, T. H., & Johnsen, F. T. (2014). *Enabling service discovery in a federation of systems: WS-Discovery case study*. NORWEGIAN DEFENCE RESEARCH ESTABLISHMENT KJELLER.

Domingo, A., & Wietgrefe, H. (2015, October). An applied model for secure information release between federated military and non-military networks. In *Military Communications Conference, MILCOM 2015-2015 IEEE* (pp. 465-470). IEEE.

Dos Santos, D. R., Marinho, R., Schmitt, G. R., Westphall, C. M., & Westphall, C. B. (2016). A framework and risk assessment approaches for risk-based access control in the cloud. *Journal of Network and Computer Applications*, *74*, 86-97.

Goldenberg, I., & Dean, W. H. (2017). Enablers and Barriers to Information Sharing in Military and Security Operations: Lessons Learned. In *Information Sharing in Military Operations* (pp. 251-267). Springer, Cham.

Łubkowski, P., Hauge, M., Landmark, L., Barz, C., & Sevenich, P. (2015, May). On improving connectivity and network efficiency in a heterogeneous military environment. In *Military Communications and Information Systems (ICMCIS), 2015 International Conference on* (pp. 1-9). IEEE.

Nasim, R., & Buchegger, S. (2014, December). Xacml-based access control for decentralized online social networks. In *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing* (pp. 671-676). IEEE Computer Society.

READ, David Scott; VAN BUREN, Scott. *System, method, and program product for lightweight data federation*. U.S. Patent No 9,984,136, 2018.

Rudack, M., Palacios-Camarero, C., & Wietgrefe, H. (2016, May). On the creation of a single mission-wide information domain in military operations: Application of the information clearing house and release gateway at NATO exercise Trident Juncture 2015. In *Military Communications and Information Systems (ICMCIS), 2016 International Conference on* (pp. 1-7). IEEE.

Suzic, B., Prünster, B., Ziegler, D., Marsalek, A., & Reiter, A. (2016, October). Balancing utility and security: Securing cloud federations of public entities. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"* (pp. 943-961). Springer, Cham.

Suzic, B., & Reiter, A. (2016, August). Towards secure collaboration in federated cloud environments. In *Availability, Reliability and Security (ARES), 2016 11th International Conference on* (pp. 750-759). IEEE.

Soeters, J. (2017). Information Sharing in Military and Security Operations. In *Information Sharing in Military Operations* (pp. 1-15). Springer, Cham.