sciendo

Land Forces Academy Review
Vol. XXVI, No 1(101), 2021

INFORMATION-SHARING CHALLENGES AND ISSUES IN MULTINATIONAL OPERATIONS, PART 2

András TOTH
University of Public Service, Budapest, Hungary
toth.hir.andras@uni-nke.hu

ABSTRACT

To share information in a multinational environment is always a big challenge. This statement is especially true when systems with different classification levels need to operate simultaneously, or different national classified systems must work together. In the first part of this article, the author analysed the different international security management procedures, the possible threats, vulnerabilities, and solutions to create the most effective information-sharing environment. The purpose of this article, as in the first part, is to analyse and evaluate the different information sharing methods and procedures that can be applied to the sharing of information between classified and non-classified networks. It also analyses the risks arising from their use and the security measures needed to remedy them. In this paper, the author collected the possible information sharing techniques and solutions and analysed the different methods to find the best result to share information in multinational environments.

KEYWORDS: air gap, content filtering, data diode, information security, information sharing

1. Introduction

In NATO and EU operations, the information always must be available at the appropriate time, place, and form. A trustworthy information environment is needed to reach this, where every member can share the information in safe circumstances. In this paper, the author reviewed pieces of literature on military information-sharing research to organise and integrate diverse studies. He collected research articles and reports across military information-sharing disciplines, including national and international (EU, NATO) doctrines, complex systems science, and theories of information-sharing techniques and solutions. To find the best result, he used SWOT analysis to determine the strengths, weaknesses, opportunities, and threats of the different methods. The analysis identified the negative and positive aspects of each solution, and further analysis of these effects distinguished possible improving solutions. The analysis identified the negative and positive aspects of each solution, and further analysis of these effects distinguished possible improving solutions. The various solutions are only possible suggestions that can be applied to tasks performed in an international environment. The author's goal was to determine if technical implementations exist that meet today's information security challenges and are suitable for multinational operations to protect data fully.

.

2. Information-Sharing Solutions in Multinational Operations

The success of NATO operations in each case depends on the operational effectiveness of the participating member

DOI: 10.2478/raft-2021-0004

states that based on adequate information-sharing capabilities. Therefore, tools and systems must comply with NATO standards and regulations and follow the procedures established in operational rules.

In 2014, at Wales's summit, NATO declared the Partnership Interoperability Initiative (PII). It includes:

- interoperability between Partner nations in NATO operations and missions in recent years has been supported and strengthened by the PII;
- PII draws attention to the importance of interoperability for all Member States and recommends that partners use new tools in their cooperation in order to create the most interoperable environment possible in NATO operations;
- an interoperability platform has also been set up by PII to enable partners to discuss interoperability issues more broadly, deepen interoperability capabilities due to future crises, and work together on a single platform.

The primary goal of NATO policies is to enable member states to work effectively and successfully to develop interoperability to achieve tactical, operational, and strategic goals. The direct result of this is that unified infrastructures and means can establish effective communication channels, sharing associated doctrines and procedures. Creating interoperability can combine NATO's and members' resources, avoid duplication of networks, and create coherence among member states. The designed environments support NATO initiatives such as Smart Defence and Connected Forces in all dimensions of interoperability, as well as the technical, procedural, and human dimensions (North Atlantic Council, 2014).

NATO disposes of an information-sharing solution among members, which called Information Exchange Gateway Case C (IEG-C) project. It provides support for information exchange services of critical information and real-time data between the NATO Secret core network (which comprise NATO commands, agencies, and connected NATO Nations) and Mission Secret networks (for NATO Responses Forces, NATO-led Coalition Exercises or Operations) (NCI Agency, 2020). However, it does not support the communication among national networks outside of NATO core; it works just in NATO systems.

To support information-sharing the Cyber Information and Incident Coordination System (CIICS) is a perfect solution. Information management and sharing in federal cyberspace are requirements for all member states and a shared severe challenge within NATO and Partners. The CIICS can create a secure environment to support multinational collaboration, decision-making, and task execution, such as the Federated Mission Network. It is an information-sharing capability designed to support C5ISR (Command, Control, Communication, Computer, Cyber, Intelligence, Surveillance, Reconnaissance) systems as well as military decision-making processes, planning, and implementation. It supports essential system requirements such as flexibility, continuous availability, and scalability, which are essential to support the multinational environment of future NATO operations. CIICS is based on peer-to-peer technology, which means no centralized resource allocation is established; the nodes communicate with each other for information-sharing. Authentication between each node is implemented using PKI, which significantly increases network security. The nodes provide access and applications for users, primarily through web interfaces. (Brown, Moye, Hubertse, Glavan, 2019). It is a good idea for information-sharing among nations, but it works with permanent nodes, there can be connection problems to them in operations and missions.

2.1. Classification Categories in Multinational Operations

The commonly used communication solutions in multinational operations are the use of national, NATO or EU networks. In this section, the author examines NATO operations. NATO has four classified information levels: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED. Both official and non-classified information are distinguished within NATO. More specifically, NATO's classification categories are defined as follows:

- COSMIC TOP SECRET (CTS) – This security classification used in the case of information if the leakage or unauthorized access of data would result in exceptionally serious damage to their stable operation of NATO and its member states.
- NATO SECRET (NS) – This security classification used in the case of information if the leakage or unauthorized access of data would result in severe damage to their stable operation of NATO and its member states.
- NATO CONFIDENTIAL (NC) – This security classification used in the case of information if the leakage or unauthorized access of data would result in damage to the interests of NATO and its member states.
- NATO RESTRICTED (NR) – This security classification used in the case of information if the leakage or unauthorized access of data would result in disadvantageous to the interests of NATO and its member states.
- NATO UNCLASSIFIED (NU) – This security classification is applied to official documents and information that belong to NATO but do not meet the above classification requirements. This information may also be accessed by non-NATO states and organizations, granted that this does not harm NATO's interests (NATO Security Committee, 2006).

During NATO operations and missions, the commonly used networks are NATO UNCLASSIFIED, NATO SECRET and MISSION SECRET (like ISAF SECRET, KFOR SECRET, SFOR SECRET, MCSI SECRET).

2.2. Information-Sharing Issues in Multinational Operations

There are many cases where it is necessary to share information between open networks and secret networks, such as sending open-source intelligence (OSINT) reports. To perform these kinds of information-sharing, to connect networks with different classifications is essential. One other issue is that the successful accomplishment of the operations always requires the support of many NGOs. These parties can be private and non-governmental organisations, as well as governmental agencies, embassies and other offices run by own or local government such as:

- local fire, police and disaster management departments;
- national and international health organisations and agencies;
- Human Rights Watch;
- Amnesty International;
- Child Concern;
- International Committee of the Red Cross;
- and press (BBC, Al Jazeera, CNN).

There are several extraordinary events during which these organisations can provide sober assistance and possibly play a leading role. These include diplomatic problems, peacebuilding and support operations, humanitarian aid, natural and industrial disasters, and refugee crisis management. Ensuring secure information-sharing during multinational operations is a crucial challenge, which poses a severe and combined challenge to all participants throughout the operation. Critical issues raised during the collaboration that may affect day-to-day operations and management include, but are not limited to, the following:

- the ability to respond quickly to problems, situations, crises from allied forces;
- the most optimal way to use resources (e.g., commercial off-the-shelf products, databases, legacy systems) to support the task without affecting its predetermined performance;
- the ability to dynamically design, manage and operate security measures and policies during multiple co-existing crises;
- all users involved in crisis management must have the appropriate access rights to information, thus ensuring compliance with security policies;
- apply security policies in accordance with federal obligations that are authorised, authenticated, valid, scalable, and can contribute to responding to arising requirements in near real-time, validating results;
- the ability to track user activity and behaviour based on predefined and established security policies (Phillips, Ting & Demurjian, 2002).

2.3. Information-Sharing Techniques in Multinational Operations

Every multinational operation is different. There are different forces, participants, tasks, and missions, as well as networks, and classification levels. Many alternative solutions exist to handle these differences, but it is usually a significant challenge to find the right and the best way to share sensitive information because of the complexity of the problems.

One of the solutions is to use the air gap. The essence of the air gap is that sensitive information and systems can be completely separated from other operating networks, especially insecure interfaces, physically, electronically, and electromagnetically. The air gap can significantly reduce the potential for compromise and disasters and greatly increase system security. Using the air gap method, the user must first connect an external hard drive authorized for the system and domains to a computer. The user copies the data to the attached hard drive and then performs a security check on the data copied to the media on a gate machine (dirty machine). These gate machines are usually equipped with five to ten different anti-virus software and other engines to detect malicious code. The advantage of the air gap solution is that our security domains, which are isolated and independent of all other networks, are not affected or threatened directly by an external network attack. This method also has disadvantages, such as copying data between different security domains takes much time. It is usually used when different nations want to share information, but they have no gateways between their networks.

When the participants in the operations use the same networks, for instance, the NATO UNCLASSIFIED and NATO SECRET ones, one right solution can be the data diode. It is possible to send information from an unclassified device to a secret one with it, but the other way is not working. With this solution, the way of the information is always one-way so that no data can leak into the lower domain. There may be a potential risk to the integrity and availability of data handled in the higher domain with network attacks, or malicious codes with the files transmitted from the lower domain (Wrona, Oudkerk & Hallingstad, 2010).

Sometimes it is needed to share information from the secured domain to the unclassified as well. It is not possible with data diodes, so we must use a solution with two-way communication. In this case, it is mandatory to use the methods as mentioned in Article Part 1, with border-protections and content filtering. The connection from the unclassified system requires traffic control, scanning incoming files for malicious code, and intrusion detection. On the other way, it is necessary to filter sensitive keywords and word fragments like secret, mission, coordinates, names. It is the easiest and fastest solution to share information between multinational troops, but it is required well-trained IT and IT-security professionals who can build and manage the necessary information security environment for the networks.

In the following, the author presents the SWOT analysis results, in Table no. 1, 3, and 5 of the solutions mentioned earlier. He tried to find the most specific advantages and disadvantages, the strengths (S), the weaknesses (W), the opportunities (O), and the threats (T) of the different alternatives and to find the best solution. The author has examined the threats of each solution with the areas, which can cause issues to the established systems and networks. The analysed areas are data leakage, data modification, infection with malicious code, and loss of information-sharing, where the numbers show the possibilities of the risk occurring (1 = not possible, 2 = possible, 3 = high probability). The results are shown in Table no. 2, 4, and 6, where the highest number indicates the highest occurrence of the threat.

Table no. 1

Air gap SWOT analysis

AIR GAP SWOT ANALYSIS	**HELPFUL**	**HARMFUL**
INTERNAL ORIGIN	S1: no network connection; S2: offline data cannot be affected; S3: requires gaining physical access before executing any sort of attack or breach.	W1: slow information-sharing; W2: social engineering (Edward Snowden – he drew attention to himself in 2013 when he leaked top-secret information about the agency's data collection, analysis, and monitoring activities as an agent for the U.S. National Security Agency); W3: malicious codes can upload to the system from portable medias; W4: easy to lose portable medias.
EXTERNAL ORIGIN	O1: no remotely access; O2: no attacks against secured network from unsecured.	T1: social engineering (quid pro quo – the basic principle of it is that attackers offer some remuneration in exchange for information, taking advantage of people's sense of reciprocity tailgating – it is a type of physical security attack in which an attacker exploits people's credulity, naivety, and thereby allows them to gain access to security areas without permission); T2: the loss of portable media can result data leakage; T3: malicious codes can upload to the system from portable medias.

SWOT analysis no. 1 shows that the main advantage of air gap is that there is no network connection, so remote access is not possible (S1, O1). Physical access is required to attack the network, but the essence of air gap is that data is shared by using portable medias, with which malicious codes can be transferred to the network and systems (S3, W4, T3). Baiting is a form of social engineering where attackers leave maliciously infected flash drive in prominent places where the potential victims can easily find it and exploiting the victims' curiosity as soon as they plug the flash drive into their machine, the malware activates itself (W2, W3, T1, T3). The main issue with air gap is that sensitive data can be leaked by influencing or blackmailing users, for example, by intentionally losing portable media (W2, W4, T1, T2).

Table no. 2

Air gap threat analysis

	T1	T2	T3	Σ
Data leakage	3	3	1	7
Data modification	3	1	1	5
Infection with malicious code	2	1	3	6
Loss of information-sharing	2	3	2	7

It is clear from the results of Table no. 2 that in the air gap, the greatest danger is caused by data leakage and loss of communication connection. The main causes of these are social engineering-based attacks as well as lost flash drives. To reduce these reasons, it is imperative to increase users' security awareness to be aware of these attacking vectors and their effects. The main advantage of the air gap is that data modification is possible just by the users; attackers cannot directly access the information.

Table no. 3

Data diode SWOT analysis

DATA DIODE SWOT ANALYSIS	HELPFUL	HARMFUL
INTERNAL ORIGIN	S1: one-way communication; S2: integrity of the secured network is preserved; S3: no jeopardising the integrity or the confidentiality of the network.	W1: one-way information-sharing; W2: portable media is needed to share information from secured to unsecured network (can be lost).
EXTERNAL ORIGIN	O1: easy to share information from the unsecured network to the secured; O2: no data leakage from secured network.	T1: malicious codes, contents (files, attachments) from the unsecured network; T2: the loss of portable media can result data leakage; T3: malicious codes can upload to the system from portable medias.

SWOT analysis no. 2 shows that the main advantage of data diode is that the information is shared in one direction so that data leakage from the protected network is not possible, and the data transfer from the unclassified network to the protected one is close to real-time (S1, S2, O1, O2). It is easy to share information from the unsecured network to the secured one, so infected contents (files, attachments) can be sent from the unsecured network to the protected system (W1, T1). Due to one-way communication, the use of a flash drive from a qualified network to a lower security network for information sharing is a problem. Using the flash medias, infected files can be transferred to the protected network, causing damage to it (W1, W2, T3). Loss of these flash drives can also be a problem, which can lead to data leakage (W1, W2, T2).

Table no. 4

Data diode threat analysis

	T1	T2	T3	Σ
Data leakage	1	3	1	5
Data modification	1	1	1	3
Infection with malicious code	3	1	3	7
Loss of information-sharing	2	2	2	6

In the case of the data diode, the biggest problem is the malicious code, which can come from unprotected networks or the flash media used. Up-to-date virus protection solutions can help avoid these vulnerabilities, and adequate policies can restrain that files on the flash drive could run automatically. Its advantage is that access to data is impossible due to one-way communication, so it cannot be modified.

Table no. 5

Content filtering SWOT analysis

CONTENT FILTERING SWOT ANALYSIS	HELPFUL	HARMFUL

INTERNAL ORIGIN	S1: two-way communication;
	S2: user independency: automatic content filtering;
	S3: easy and fast information-sharing.
		W1: limited content analysis: the filter can capture important information;
		W2: automatic content filtering: user inattention.

EXTERNAL ORIGIN	O1: no malicious codes, contents; O2: easy and fast information-sharing.	T1: possible remotely access; T2: possible attacks against secured network from unsecured.

The main advantage of the content filtering is that the connection based on two-way communication which provides easy and fast information-sharing (S1, S3, O2). Automatic content filtering makes users' work easier, which may be inattentive as a result and this makes it easier for users to skip over the signs that they may have been the victims of an attack (S2, W2, T1, T2).

Table no. 6

Content filtering threat analysis

	T1	T2	Σ
Data leakage	3	2	5
Data modification	3	2	5
Infection with malicious code	1	1	2
Loss of information-sharing	3	3	6

The biggest advantage of content filtering is that data and systems cannot be infected with malicious code, as known viruses are constantly filtered. Users cannot share sensitive data; however, if an attacker succeeds in gaining access to the system, the security settings applied may no longer prevent the data leak.

When analysing the different alternatives, the main result found is that there is no right solution. At the air gap, social engineering is the most significant disadvantage. With adequate information security awareness, the risk can be reduced, but the users' habits can be a big issue during this solution. The data diode is a good alternative if it aims to share information from the unsecured network to the secured one. At the other direction, to use portable media for information-sharing is unavoidable so that it can have the same problems as the air gapping. The two-way communication solution is inescapable to avoid the use of portable media. In this case, the central dilemma is that there is a gateway between the networks so that attackers can reach the secured system from the unsecured.

One common issue is the malicious codes and contents. One of the essential elements of protection against malware is applying a complex, advanced anti-malware solution that ensures that the information that enters the protected network does not contain any viruses, worms, trojans, and other malicious code. It is used in the content filtering, so with proper security management, there is the lowest risk of this type of attacks at this solution.

To find a more effective alternative, the author made a complex analysis, as shown in Table no. 7. This solution uses data diode from the unsecured network to the secured one, on the other way there is the air gap; and in both directions, there is the use of advanced threat protection with multiple advanced anti-malware software.

Table no. 7
Complex solution SWOT analysis

COMPLEX SOLUTION SWOT ANALYSIS	HELPFUL	HARMFUL
INTERNAL ORIGIN	S1: user independency: automatic content filtering; S2: integrity of the secured network is preserved; S3: no jeopardising the integrity or the confidentiality of the network.	W1: portable media is needed to share information from secured to unsecured network (can be lost).
EXTERNAL ORIGIN	O1: no malicious codes, contents; O2: easy to share information from the unsecured network to the secured; O3: no data leakage from secured network; O4: no remotely access; O5: no attacks against secured network from unsecured.	T1: social engineering (quid pro quo, tailgating).

With this solution, the information leakage, and the possibility of compromise of sensitive data can be reduced, but the users can willingly or unwillingly release information (S1, S2, O3, O4, T1). To avoid this, it is always mandatory to do security awareness, network- and information security trainings. Data loss or compromise by operators cannot be reduced by 100 %, but users can recognize incidents in their environment after these trainings.

3. Conclusions

There are several solutions for sharing information in multinational operations, but users must fully comply with the requirements laid down in regulations in all cases. There is no perfect solution, but adequate information security awareness can reduce the data leakages, losses, and compromises.

It is always a big challenge to find the best way to share information between national and international networks. Every nation has different security strategies, doctrines, and regulations, so the first thing that the connection points between them must be defined. When it is specified, which information with different classification level can be shared, it is needed to use the right way for the sharing. There is no 100 % solution to this; unfortunately, attackers have a very wide spectrum of attacking vectors that can be used to find vulnerabilities in systems and exploit them. To reduce the chances of this, the author analysed a complex solution in Table no. 7 that could be applied in an international environment. The solutions used in it can be found mostly in, for example, NATO operations, but they should be used not only in federal but also in other multinational tasks to protect sensitive data. With this solution, the numbers of disadvantages are the less, reducing the data leakages, losses and compromises.

It is also needed to use well-organised and well-managed administrative and physical security solutions to avoid social engineering attacks and data leakage.

Acknowledgements

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-20-5-NKE-5 New National Excellence Program of the Ministry of Innovation and Technology

REFERENCES

Brown, S., Moye, T., Hubertse R., & Glavan C. (2019). Towards mature federated cyber incident management and information sharing capabilities in NATO and NATO Nations. *IEEE Military Communications Conference (MILCOM) Norfolk, VA, USA*, ISBN: 978-1-7281-4280-7.

NATO Security Committee. (2006). *Directive on the security of information, AC/35-D/2002-REV2*, available at: https://www.statewatch.org/news/2006/oct/nato-2005-class-info.pdf, accessed on 28 March 2020.

NCI Agency. (2020). *Provision of Information Exchange Gateway (IEG-C) between NATO Secret and Mission Secret domains project.* IFB-CO-14314-IEG-C, NCIA/ACQ/2020/6225.

North Atlantic Council. (2014). *Wales Summit Declaration*. Paragraph 80-82, 86-89.

Phillips, C., Jr. Ting, T.C, & Demurjian, S. (2002). Information Sharing and Security in Dynamic Coalitions. *SACMAT02: 7th ACM Symposium on Access Control Models and Technologies Monterey California USA.*

Wrona, K., Oudkerk, S., & Hallingstad, G. (2010). Designing Medium Assurance XML-Labelling Guards for NATO. *IEEE Military Communications Conference (MILCOM) San Jose, CA, USA,* ISBN: 978-1-4244-8178-1.