sciendo

Land Forces Academy Review
Vol. XXV, No. 4(100), 2020

INFORMATION-SHARING CHALLENGES AND ISSUES IN MULTINATIONAL OPERATIONS, PART 1

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

ABSTRACT

One of the essential prerequisites for an efficient and effective organisation in our information society is the timely provision of information to the entitled person or persons. This is particularly important in the public, economic and business sphere, in public administration, law enforcement agencies and military operations as well. The information must always be available in the right place, at the right time, in the required quantity, quality and format, in order to gain and maintain the information superiority. This paper aims to analyse and present the methods of information sharing among different classified and non-classified systems and networks, their proposed areas of application, the security measures required for their safe implementation, and the risks and issues arising from their use. In this part of the article, the author analysed the different international security management procedures, the possible threats, vulnerabilities and solutions to create the most effective information-sharing environment.

KEYWORDS: data leakage, information security, information sharing, malware, network attacks

1. Introduction

In our information society, one of the primary conditions for efficient and effective military operation is that the information provided to the entitled person or persons promptly. Information management includes the assessment and planning of operational needs, the information gathering or production; the storage and maintenance; distribution, the information sharing and utilization of resources. Information sharing with authorized persons within the organization or with cooperating parties, whether foreign partners or international organizations, is an essential condition for an organization to operate efficiently and successfully. In all military operations, the main goal is gaining and maintaining information superiority, which is the fundamental key to success. In NATO and the EU, there are several technical solutions for the interconnection of systems that handle "unclassified" data or data with different classification levels, which have also been accepted by supervisory bodies and authorities, so the requirements for their safe operation have laid down in different directives.

In many cases, it is required to process open-source information on a classified electronic information system so that the data flow in the opposite direction cannot take place. It may also be necessary to move data files between electronic information systems that handle data of the same or different classification levels. Even more impressive is when the data processed on these systems have different entities, such as national or foreign.

DOI: 10.2478/raft-2020-0037

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.

2. Methods

The author reviewed military information-sharing research literature to collect and organise various relevant studies. He collected research articles and reports across military information-sharing regulations and rules, including national and international (EU, NATO) doctrines and theories of information-sharing techniques and solutions. There are hundreds of relevant literature on the above topics, but the scope for summarising them in a comprehensive study is very narrow. To create a prospective smaller subset and framework, the author used the following research methods. Firstly, he used the software Harzing's Publish or Perish to find, collect, and analyse military information-sharing publications on Elsevier Scopus. He used Scopus as his chosen repository, due to the significant amount of relevant information security literature in its database. He also used Google Scholar, where he could even find military books, reports, and articles that are not indexed in other academic search engines. Using sub-sets during the searches, he still got more than a hundred results, but after he compared them to see duplicates and finally he got a final combined list of 25 records. Analysing these results, he could specify the doctrines, rules, and frameworks of information sharing. He also could do a comparative analysis according to the different national and international processes; he found the best solutions for multinational operations.

3. International Information Security Management

Information security, often abbreviated as InfoSec, refers to activities, processes, procedures, and tools designed to protect sensitive information from external access, eavesdropping, eventual modification, destruction, or theft. Attackers typically aim to gain unauthorized access to information, causing material damage or severe damages to business continuity, availability. Thus, information security means the set of practical activities that protect data and systems of individual organizations, companies, and governments against external attacks. You can see the different domains conducting information security in Table no. 1.

Table no. 1

The different domains within the term information security

Information security domains	
Communications Security	Protection against possible attacks on the information system and other threats that may lead to changes in the characteristics of the technical infrastructure that do not meet the requirements set by the system administrators.
Operations Security	Protection against manipulation of work processes and procedures, thus preserving the planned operations.
Information Security	Protection against theft, modification and destruction of data collected, processed, stored and transmitted in the information system.
Physical Security	Protection against physical attacks affecting the operation of the information system. Excellent examples include direct access to servers, insert malicious hardware into the network, and forcing users to do physical damage.
Public/National Security	Protection against threats from cyberspace with political, military or strategic benefits, executed with physical or cyber assets.

(adapted from European Network and Information Security Agency, 2015)

Security agreements regulate the exchange and sharing of classified data with other countries, and international organisations concluded between the parties. All NATO and EU member states are entitled to handle and share NATO and EU classified information with NATO and EU organizations based on security agreements, and to share and manage national classified information with other NATO and EU member states prepared for the benefit of NATO and the EU. In 2003, the Agreement between the European Union and the North Atlantic Treaty Organization on the security of information entered into force, and it formulated, that each Party shall:

It must protect and safeguard classified information or material provided or exchanged by the other Party.

It must ensure that the classified information or material provided and transmitted retains its level of classification throughout the process. The receiving Party shall handle, store and process the received classified information in accordance with its own security regulations under the classification level.

It is prohibited to use classified information for other purposes than specified by the originator and for which it was provided and exchanged.

It is forbidden to share classified information with third parties without the permission of the originator.

It also specified that each Party should have security organizations and programs based on common security principles and minimum standards. These standards should be integrated into the Parties' security systems to ensure that security levels are equivalent at all the Parties to protect classified information and material.

According to the security agreements among NATO and its member states, the Parties shall protect and safeguard classified information originating from NATO, provided to NATO by a member state, or transferred from one member state to another in support of a NATO mission, program, project or contract (EUR-Lex Document 22003A0327(01), 2013).

Examining the above, it can conclude that there is no regulation on the types of information sharing where a NATO member wishes to share classified information with another NATO member without doing so in the interest of NATO. In these cases, countries must sign a bilateral or multilateral security agreement with each other. These security agreements between nations only regulate the security requirements of classified information sharing in general. Still, they include the details of the information sharing and the rules for the interconnection of electronic information systems. Members may only share classified information in a strictly regulated, supervised manner, with the mutual consent of the cooperating parties, and it always based on a complex risk analysis.

4. Information Security Threats and Solutions

Member states must design the IT system handling electronic classified data by the relevant NATO and EU requirements and legislation. Accreditation of the subnetwork and guaranteeing compliance with federal (international) requirements is always the responsibility of the participating nations. The next step is the verification and certification of the technical system providing the interconnection (technical design, regulation and supervision issues) by the competent international organisation. Tasks related to interconnection or connection to other networks may occur during exercises, relocations or demonstrations both at home and abroad. The members shall develop the electronic information security requirements, security policies and procedures required for interconnection (or connection) following

DOI: 10.2478/raft-2020-0037

NATO, EU or other international requirements, including hardware and software certification requirements. The IT systems with the accredited hardware and software configuration and external data exchange services can only operate at the location specified in the data management license. According to NATO, EU and national requirements, the members, the organisations and departments must use encryption in all cases where the transmission of RESTRICTED or higher electronic data crosses the border of the protected area (Kassai, 2015).

During the information sharing between different security domains, it is always mandatory to be placed great emphasis on protection against malicious codes, prevention of data leakage between security domains, and timely detection and prevention of attacks from the "outside world".

4.1. Malware Protection

Malware is malicious software that acts against the interests of users, performing malicious activities on data and devices without their knowledge. Malware can also affect any network element with which an infected machine can communicate.

Malware includes simple computer worms, trojans, as well as very complex spyware and ransomware programs. Malware always needs a communication channel through which they can spread and a code by which they can perform the malicious activity.

To share information securely, one of the essential tasks of border protection systems – located and operating between security domains – is to protect against the malware listed in Table no. 2 (RedHat, 2018).

Table no. 2

Types of malware

Delivery tools	Payloads
Trojan horse: It prompts the user to install it **Worm**: It multiplies itself	**Adware**: Advertising software that is usually installed either as a trojan or as part of free versions of commercial programs **Botnet**: An attacker-controlled army of computers **Cryptocurrency miner**: It utilizes the computing capabilities of computers for cryptocurrency mining **Ransomware**: Trying to extort money from its victims – by paying a ransom **Spyware**: It leaks information about the user's machine without the knowledge or allows others to do so **Other damage**: Data destruction, vandalism, sabotage
May be combined with: **Exploit**: It exploits software vulnerabilities to gain access to systems and devices **Phishing**: It prompts the user to issue user's access data **Rootkit or bootkit**: They facilitate the acquisition of administrator privileges to achieve greater management and control goals	

(adapted from RedHat, 2018)

The design of the protection, as well as the reduction of threats to systems and data, is worth dealing with in a complex way, and Advanced Threat Protection (ATP) developing is recommended. ATP includes security solutions that can provide combined protection against attacks on sensitive data. It allows protecting the networks and systems against sophisticated hacker attacks such as:

●bait and switch – illegal advertising of goods that allow the replacement of more substantial, more expensive or more inadequate quality products at affordable prices;

●SQL injections – a code injection technique against data-driven applications, and it can result in unauthorized access to sensitive data, such as personally identifiable information, passwords, or credit card details;

●cryptojacking – the hijacking of third parties' computer to mine and move cryptocurrency;

●DDoS attacks – attacks the known weaknesses of a specific (server) application or operating system, or the properties (weaknesses) of a unique protocol, with the aim of entirely or partially disabling an IT service, diverting it from its correct operation.

●Advanced threat protection has three fundamental goals:

●early detection (detect potential attacks and threats before they provide access to networks or sensitive data wanted to protect);

●adequate protection (the possibility of applying complex protection mechanisms and procedures after detection);

●and response (ability to react immediately when an attack occurs, reduction of damage caused, the immediate start of recovery).

To achieve the above goals, each ATP service must have the following components, elements, features, and solutions:

●Real-time visibility: Continuous monitoring and visibility are essential for real-time threat detection. Attacks that have already taken place are significantly more costly than developing an appropriate real-time visibility solution.

●Context: To achieve adequate security effectiveness, suspicious activities should be analysed in the context of all checkpoints and prioritise the events that pose the greatest threat to the protected system. Once a critical threat has identified, it quickly can be quarantined and isolated to prevent further incidents.

●Data awareness: Users at all levels must be aware of the data they manage, its sensitivity, value, and other factors that can help identify potential threats that can cause severe damage to this data and contribute to appropriate responses (Lord, 2020).

●ATP solutions must include at least the following protection measures:

●use of predefined and enabled file formats;

●use of multi-engine virus scanning (for example gate machine);

●sanitization of data.

Regulatory tasks include that during information sharing, collaborating parties must predefine all file formats that will be allowed when sharing information between different security domains. Particular attention should be paid to the settings of our border protection system so that malicious programs cannot enter our system during the security check with data created in a file format that is not allowed. The system must detect in time and prevent if, for example, an attacking file tries to enter malicious code into our system.

When sharing information between security domains, it is advisable to use gate machines that have several malicious code search engines (multiscanning system) at the same time. Different antivirus engines use different algorithms to analyse files, and various vendors have different antivirus databases, which increases the chances of detecting malicious code. Virus scanning should also cover compressed files (OPSWAT, 2020).

4.2. Data Leakage

Another critical task of the border protection system in information-sharing between security domains is to prevent data leakage. This prevention is especially crucial for qualified data management systems, where data confidentiality is a priority. Data Loss Prevention (DLP) policy use is recommended as part of the border protection system to detect and prevent leakage of electronic data. DLP devices can check for data leakage in three ways, depending on where the data occurs:

●data at rest (stored data): a set of information stored in databases, cloud repositories, computers, portable devices, and other storage locations;

●data in motion: the process of sending and receiving data (for example, during intelligence, surveillance and reconnaissance report sending);

●data in use – a set of data that users are currently working on, modifying, or reworking.

●DLP systems can provide:

●the ability to control access to information systems and devices;

●the ability to monitor all activities that take place on networks, servers and workstations, whether they were successful or not. These include writing, reading, modifying, deleting files;

●the ability to control all information flows, including data sharing within and outside the organization, and check the sending and receiving information from mobile or IoT devices from remote locations;

●the ability to control the number of information sharing channels, thereby blocking the ability to stream and possibly eavesdrop on outgoing communication channels.

Administrators can configure DLP devices in several ways to notify if a data leak is detected. For example, you can send an alert to the organization's security operations centre (SOC) and/or inform the user via email of a policy violation. The DLP solutions work with the process, which might proceed like the following:

●identification of incidents based on defined rules;

●blocking outgoing messaging and information sharing according to established policies;

●creating an event report that contains all information about the event and sends it to a predefined email address, such as the chief information security officer, or stores it in a secure database on an internal data store by DLP policy (Melnick, 2019).

A data diode can be used to prevent data leakage. The data diode is based on the principle of a conventional diode. This protection device provides only one-way communication from a lower security rating range to a higher one and does so by preventing data leakage from the high range to the low range. A data diode is a network hardware tool that placed between two networks with different security levels to control the flow of information. With this cybersecurity solution, the information can flow only from one system to another, and opposite communication is not possible. This unidirectional flow of information guarantees that the integrity and confidentiality of sensitive information are not compromised and compromise can rule out, as data from a higher security level cannot enter the lower security level network. This solution allows information to transfer without compromising the system. The significant advantage of the data diode is that it is hardware and not software-based, so it cannot be attacked by malicious code, making it even more resistant to intrusions (Advenica, 2019).

During information-sharing, we can also use content filtering, which may be hardware or software solutions. Content filtering is an automated system that processes a large amount of data and takes action when any content that meets certain conditions is detected. These hardware and/or software solutions can be configured to filter entire domains, specific URLs, keywords, word fragments, images, and ports. Network traffic between different security domains is provided by proxy servers, which can be an additional security level, segment (Figure no. 1). The electronic information system uses authenticated proxy servers to direct internal communication traffic on the managed interfaces to the specified external networks. The proxy server not only controls the data flow but is also able to analyse the data traffic.

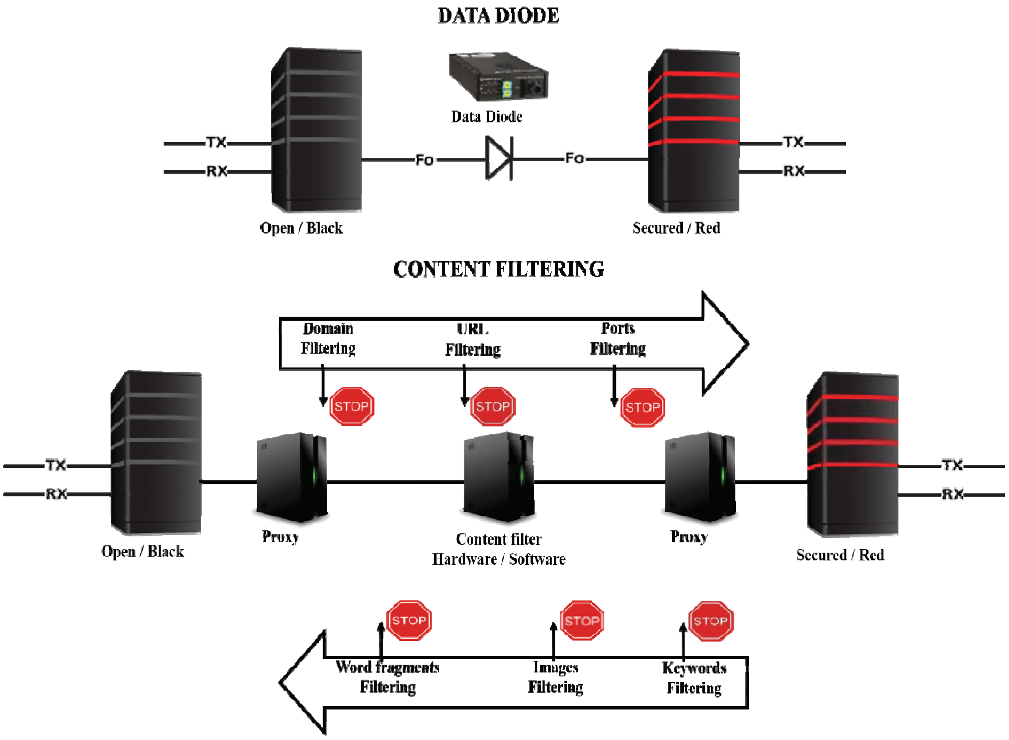

Figure no 1: *Data loss prevention solutions*
(Source: Koumartzis & Veglis, 2011)

Most of these solutions are software-based and run on servers that use mirrored network ports connecting to networks. It is also an excellent solution to install dedicated devices at the same time as installing the system, ensuring network traffic monitoring and controlling. They can also respond quickly to the illegal use of unauthorized and malicious content. Fundamental policies using content filtering:

- preparation of a well-planned and deliberate usage policy;
- explaining usage policy to each user and keeping them up-to-date with changes;
- carrying security awareness training on the network, computer, and application threats and security solutions;
- placing monitoring means to record and report issues with the network;
- installing mechanisms to monitor, filter, and block terms, word fragments, images, ports, URLs specified in the network policy;
- take appropriate action in all cases, when complaints are registered, or the directives violated, or the protection devices recognise any threat (Vacca, 2009).

Because this application can perform very in-depth automated analysis according to predefined rules, NATO also prefers to use it to monitor data entry and exit. It can be used, for example, when NATO classified information is transmitting as an e-mail attachment. The content filter then examines the classification level in the attached document and the header of the letter and checks whether the selected recipient has the appropriate authority to access the classified information.

A well-configured mail filter is capable of in-depth scanning and control of data traffic, even with a very complex set of information sharing criteria.

4.3. Protection against Network Attacks

Attackers typically connect to the infected computers from outside of the attacked electronic information system. Well-configured border protection devices should use to examine unusual network traffic, and with them, administrators can perform logging tools, and they are suitable for intrusion detection. During information-sharing between security domains, traffic must be separated from all other network streams. Network traffic between security domains can only and exclusively take place through the border protection systems. All other data traffic bypassing the border protection systems must be blocked.

In all cases, system administrators must install appropriate border protection systems in a demilitarised zone (DMZ) created between the security domains. The purpose of it is to allow the external attackers to access only the services and equipment located in this border zone and not to the entire network of the organisation. The DMZ can be a primary line of defence for systems that protects internal sensitive data and valuable hardware and software from unauthorised external access, potential attacks. DMZ is an essential element in the design of multilayer lines of defence, which significantly increases the security level of networks and systems. Their application is vital to ensure the protection of all elements of the system. The essential feature of DMZs is that firewalls operate at their boundaries, thus separating security domains. Proxy servers can also be installed in the DMZ by increasing controllability and log ability by using administrative control and the cache service. The traffic passing through them is controlled and managed by routers with traffic filtering and other firewall capabilities. The three essential types of firewalls are the following:

●Static packet filters: Its basic principle of operation is to control the data packets flowing through it among terminals, servers and the network using network interfaces, IP addresses and ports control. It checks that the contents of the packages comply with the rules as specified in the network policy. If any abnormality found, the packet is blocked and not allowed into or out of the network.

●Dynamic packet filter: This filter continuously monitors the state of established connections and blocks packets that in some way negatively affect the state of the connections. It characterized by the fact that only the necessary ports are open for the time of the traffic and only for the addressed traffic, the others remain closed. On the firewall, there is a status table for each connection, and the traffic through the established link is monitored, and recorded in this status table. An external packet can only go through the firewall if it belongs to a dedicated connection and has the status corresponding to the entry.

●Application-proxy gateway: An application-level firewall represents an entirely different concept compared to packet-filtering firewalls; it separates various networks by using network address translation (NAT). It is designed to preserve IP addresses, and its primary function is that network devices with unregistered IP addresses used on the internal network can communicate towards the Internet by translating internal private addresses into globally unique addresses. While packet filters are general-purpose tools for managing all network traffic, application-level firewalls are designed only to filter unusual network traffic for one or more applications. Most of these firewalls include the software and proxy service used for that application. A proxy service is a special-purpose program that manages traffic for given protocols within a firewall. The proxy server does not allow a direct connection between the client and the real server (Rababah, Zhou & Bader, 2018).

To increase the security of network traffics, an adequate solution is the use of public key encryption and authenticating the servers and border protection devices involved in information-sharing. It can be used when someone must send sensitive information on an unsecured network. In public key cryptography without any sharing of secret key sender and receiver are perform secure communication over the unsecured network. Public key cryptography based on asymmetric encryption, which uses two keys, which is a fundamental difference from symmetric encryption, which uses only one key for both operations. One key required for encryption and the other needed for decryption. Because each participant in a public key cryptographic system has two keys, there is no need for interaction between participants before exchanging encrypted text or data. One key is called a private key, and the other is called a public key. The secret key remains hidden, but the public key can be published. Public key cryptography is versatile and allows the implementation of essential services such as secret content management and the user or data authentication.

Public Key Infrastructure (PKI) is the combination of hardware, software, and user policies that uses asymmetric key pairs for the creation, verification, management, and secret or authentic communication of electronic signatures, including the underlying institutional system, various service providers, and devices. It's essential task is to create, issue, publish, manage and revoke the public keys required for digital signatures. The main advantage of PKI is that it provides a complete infrastructure for creating, distributing, managing, and storing digital certificates (public and private keys) (Verma & Agrawal, 2013).

5. Conclusion

There are several solutions for sharing information in multinational operations, but in all cases, users must fully comply with the requirements laid down in regulations. In this article, the author studied the different solutions to defend the information in a multinational environment. Everybody in the deployed and used networks must strive for the best solutions. Unfortunately, there is no perfect solution; the attackers can find a way to enter our systems with malware or exploiting bugs, back doors and open ports. There are software and hardware-based solutions to protect classified information. One of them can be the use of data diodes to counteract the information sharing from the higher security level network to the lower one. With content filtering, it is possible to prevent sensitive information sharing with non-authorised people. The use of a demilitarised zone can also reduce the possibility of an attack, but it is always mandatory to use encryption with these solutions to protect the information.

REFERENCES

Advenica. (2019). *What is a data diode and how does it work?* available at: https://www.advenica.com/en/blog/2019-02-19/what-is-a-data-diode-and-how-does-it-work.

European Network and Information Security Agency. (2015). *Definition of Cybersecurity, Gaps and overlaps in standardisation V1.0*. Greece: Author.

EUR-Lex Document 22003A0327(01). (2013). *Agreement between the European Union and the North Atlantic Treaty Organization*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0327(01)&from=EN

Kassai, K. (2015). Elektronikus információbiztonsági alapismeretek a honvédelmi szervezetek által kezelt minősített adatok biztonsága érdekében, *Hadmérnök, Vol. X, No. 1*, 210-223.

Koumartzis, N., & Veglis, A. (2011). Internet regulation: The need for more transparent Internet filtering systems and improved measurement of public opinion on Internet filtering. *First Monday, Volume 16, Number 10*, 1-17.

Lord, N. (2018). What is Advanced Threat Protection (ATP)?, *Digital Guardian*, available at: https://digitalguardian.com/blog/what-advanced-threat-protection-atp.

Melnick, J. (2019). 10 Best Practices Essential for Your Data Loss Prevention (DLP) Policy, *Netwrisk*, available at: https://blog.netwrix.com/2019/07/16/10-best-practices-essential-for-your-data-loss-prevention-dlp-policy/.

OPSWAT. (2020). Multiscanning, Advanced Threat Prevention with Simultaneous Anti-Malware Engines, available at: https://www.opswat.com/technologies/multiscanning

Rababah, B., Zhou, S., & Bader, M. (2018). Evaluation the Performance of DMZ. *International Journal of Wireless and Microwave Technologies, 2018-1, Vol. 8, Issue 1*, 1-13.

RedHat. (2018). *What is malware?* available at: https://www.redhat.com/en/topics/security/what-is-malware.

Vacca, J. (2009). *Computer and Information Security Handbook. Burlington*. USA: Elsevier.

Verma, R., & Agrawal, S. (2013). Data security for any organization by using public key infrastructure components and MD5, RSA algorithms. *International Journal of Research in Engineering and Technology (IJRET), Vol. 2, Issue 5.*