On the Sharing of Cyber Security Information

Eric Luiijf, Marieke Klaver

▶ **To cite this version:**

Eric Luiijf, Marieke Klaver. On the Sharing of Cyber Security Information. 9th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2015, Arlington, VA, United States. pp.29-46, 10.1007/978-3-319-26567-4_3 . hal-01431012

HAL Id: hal-01431012
https://inria.hal.science/hal-01431012v1

Submitted on 10 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 3

ON THE SHARING OF CYBER SECURITY INFORMATION

Eric Luiijf and Marieke Klaver

Abstract The sharing of cyber security information between organizations, both public and private, and across sectors and borders is required to increase situational awareness, reduce vulnerabilities, manage risk and enhance cyber resilience. However, the notion of information sharing often is a broad and multi-faceted concept. This chapter describes an analytic framework for sharing cyber security information. A decomposition of the information sharing needs with regard to information exchange elements is mapped to a grid whose vertical dimension spans the strategic/policy, tactical and operational/technical levels and whose horizontal dimension spans the incident response cycle. The framework facilitates organizational and legal discussions about the types of cyber security information that can be shared with other entities along with the terms and conditions of information sharing. Moreover, the framework helps identify important aspects that are missing in existing information exchange standards.

Keywords: Information sharing, cyber security, resilience, incident management

1. Introduction

Modern society and citizenry rely on the continuous and undisturbed functioning of critical infrastructure assets that provide vital goods and services [4]. The failure of a critical infrastructure can seriously impact the health and well-being of citizens, the economy and the environment, and the functioning of governments. Examples of critical infrastructures are power grids, transportation systems, drinking water treatment and distribution systems, financial services and government administration. These infrastructures increasingly depend on information and communications – or so-called "cyber" – technologies. Cyber security and resilience are, therefore, critical topics for modern society [2]. The timely sharing of cyber security information between organizations – in a critical sector, across sectors, nationally or internationally – is widely recog-

nized as an effective means to address the cyber security challenges faced by organizations, especially those that are part of a critical infrastructure. For example, the sharing of information across organizations at the boardroom level is stimulated by the World Economic Forum [19, 20]. Another example is the European Network Information Security (NIS) Platform, which promotes collaboration and information exchange between stakeholders from the private and public sectors [6].

The notion of "sharing" cyber security information is often misunderstood. As a result, it may create internal organizational and legal barriers to sharing information with other organizations. To address the problem, this chapter presents an analytic framework for information sharing. A decomposition of the information sharing needs with regard to information exchange elements is mapped to a grid whose vertical dimension spans the strategic/policy, tactical and operational/technical levels and whose horizontal dimension spans the incident response cycle [7]. The mapped elements facilitate discussions about the types of information that can be shared with other organizations and the conditions under which they can be shared. The time criticality of the elements, if it exists, is a factor that may influence sharing decisions. This chapter explains how existing standards for information exchange as well as standards under development are mapped to the elements. It also shows that a number of information sharing elements are not supported or even mentioned by standards or standardization efforts.

2. Definitions

A critical infrastructure (CI) consists of assets and parts thereof that are essential to the maintenance of critical societal functions, including the supply chain, health, safety, security, economy or social well-being of people [4]. Similar national definitions and sets of national critical infrastructure sectors can be found in [3].

Cyber resilience is the ability of systems and organizations to withstand cyber events. It is measured in terms of the mean time to failure and the mean time to recovery [20].

Cyber security constitutes the safeguards and actions that can protect the cyber domain, both in the civilian and military realms, from threats that are associated with or that may harm the interdependent network and information infrastructures in the cyber domain [5].

3. Previous Work

The increased focus on cyber security has demonstrated that information sharing is a very important good practice for improving cyber security across collaborating organizations. Although information sharing has proved its value in practice, little work has been done on the theoretical and practical aspects. This section discusses some of the earlier studies that provide the foundation of the research described in this chapter.

MITRE has developed a set of technical/operational-level standards for uniquely classifying and identifying threats, vulnerabilities and assets, and for exchanging intrusion detection data (e.g., [13, 14]) in order to speed up the prevent-detect-respond cycle. However, the wider incident management cycle and the tactical and strategic levels are not (yet) fully covered by these efforts.

From 2008 through 2012, a NATO Research and Technology Organization (RTO) Research Task Group focused on developing a common operating picture of coalition network defense [1]. To ease the effort, the task group emphasized the need to identify possible information exchange elements. Information exchange classes and elements within the types, specifically aimed at the defense of coalition networks, were outlined during a brainstorming session. The final report of the task group is yet to be published; only a draft final report exists that contains an initial set of ten information exchange classes and thirty-nine elements.

Research by the authors of this chapter has extended the initial set of information exchange classes and elements to the exchange of cyber security information between military entities and/or non-military coalition partners, as well as to information exchange in civilian settings. One information exchange class (actor information) and twelve new elements were added to the original set. Some of the new elements were identified after mapping the set of elements to the analysis framework, which is outlined in its final form in Section 4. This chapter uses the expanded incident management cycle as one axis of the grid to map the information exchange elements. The cycle, which is described in the National Cyber Security Framework Manual (NCSFM) [7], comprises several phases: proaction, prevention, preparation, incident response, recovery and aftercare/legal follow up.

4. Analytic Framework for Information Sharing

This section describes the analytic framework for information sharing.

4.1 Information Exchange Classes and Elements

Detailed descriptions of the cyber security information exchange classes and elements are provided in the Appendix. The information exchange classes range from technical data on incidents (Class I) and detection data (Class D) to background and context information (Class B) and good practices (Class G). Each class comprises a set of information sharing elements. Note that the classes and elements differ by the type of stakeholders that they aim to reach, ranging from cyber security operations specialists to policy makers. The stakeholder aims form the basis of the vertical dimension of the analysis framework.

4.2 Framework Levels

Based on the NCSFM governance model [7], the sharing of cyber security information takes place at three levels: (i) combined strategic and policy making

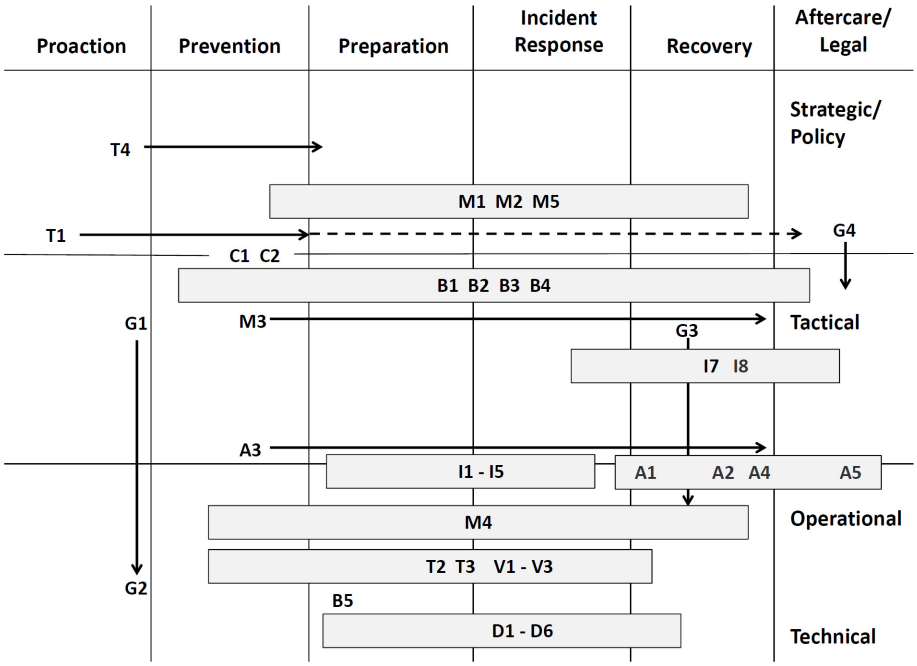

Figure 1. Analytic framework (grid from [7]).

levels; (ii) tactical steering level; and (iii) operational/technical levels. The level at which cyber security information is shared largely depends on the job positions and responsibilities in an organization. Information sharing usually takes place horizontally within the same decision making level when the information exchange is cross-organizational or cross-sectoral. Horizontal information exchange may involve the sharing of data at the original level of detail, although, in general, some form of anonymization or aggregation is employed. Shared information can also propel vertically, but then the information is usually (and preferably [8]) exchanged internal to an organization. Vertical information exchange generally involves a form of analysis in which more detailed data is aggregated and/or assessed in support of decision making at the higher levels.

4.3 Incident Management Cycle

Information sharing is a cross-mandate that spans various public and private mandates as outlined in the NCSFM [7]. Based on the incident management cycle outlined in the NCSFM, it is clear that an information sharing activity may span one or more phases of the cycle. The cycle comprises several phases: proaction, prevention, preparation, incident response, recovery and aftercare/legal follow up. For example, an organization may decide to concentrate on sharing information about proaction and prevention activities given the mandates of

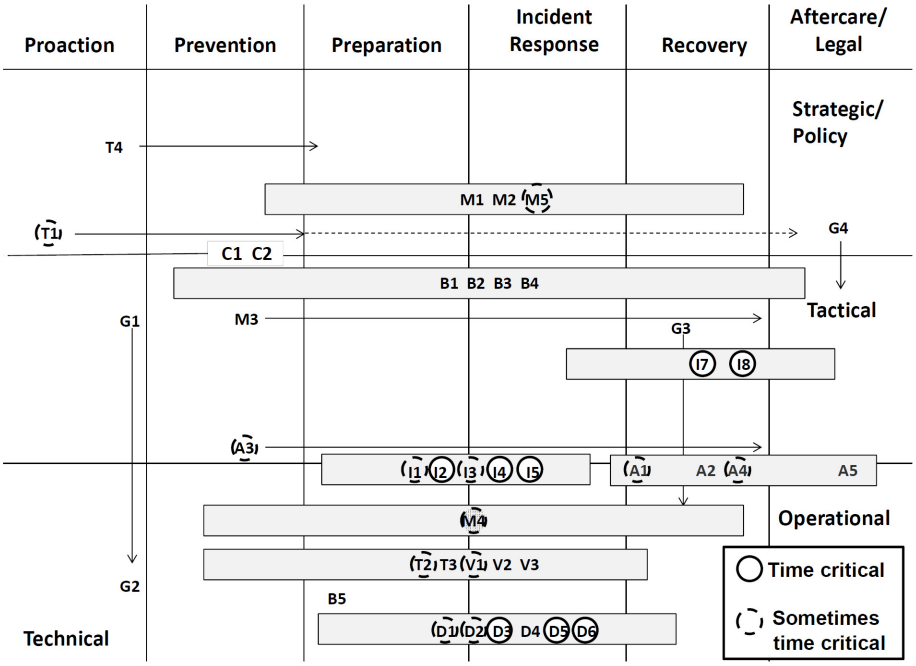

Figure 2. Time criticality of the information exchange elements.

the participants. Other sharing communities (e.g., CERT) focus on sharing incident response and recovery information. Finally, law enforcement may concentrate on collecting shared intelligence to disrupt and prevent incidents from occurring, or on deriving incident-specific evidence and situational information for criminal investigations and eventual prosecution.

4.4 Mapping the Elements to the Grid

The combination of the incident management cycle described in Section 4.3 and the three decision making and activity levels described in Section 4.2 results in a grid that constitutes the background of Figure 1. The 41 information sharing elements of nine information exchange classes are mapped to the grid. Note that the R* and S* military information exchange classes and the I6* elements are not described in this chapter.

Each information sharing element has different properties in terms of dynamics, time frame, amount of information, complexity of information, factual or weak indication, etc. Figure 2 shows the outcome of the analysis of the time criticality of the information sharing elements. Note that the most time critical information concerns the detection/incident response part of the incident management cycle. The sharing of detection data is most valuable when shared

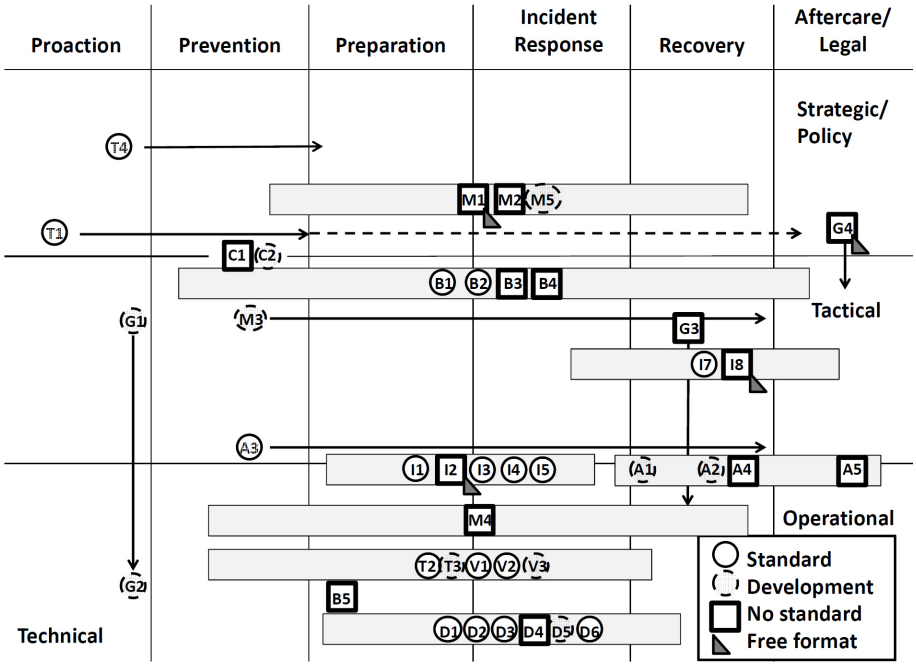

Figure 3. Standards and standardization efforts mapped to exchange elements.

promptly, preferably as enriched actionable data, in order for other organizations to be able to act on the information [8].

5. Standards and Standardization Efforts

Certain information elements can be exchanged during face-to-face meetings or via voice communications. The decision partly depends on the time criticality of the information that is to be shared [8]. Other information sharing elements can or must be exchanged via electronic means (e.g., because of time criticality or the amount of information to be shared). Simple information can be exchanged in free format (e.g., via unstructured emails). The exchange of more complex information requires structured exchange mechanisms, in other words, using standardized methods. As part of this research, mappings were performed for each element to existing standards (if any) as well as to *de facto* standards and to other efforts that may partially satisfy the needs of an identified information exchange element. Table 1 in the Appendix provides details of the mappings. Figure 3 shows the mappings to the analysis framework grid.

The analysis shows that:

- Most information exchange standards target the detection and incident response phases, and the technical/operational levels. This agrees with the statement on time criticality, which also shows that the sharing of de-

tection and incident response data is most valuable when shared promptly. Prompt information sharing requires a uniform and efficient approach as well as clear definitions of the data to be exchanged as reflected by the development of standards.

- Some standards target the sharing of strategic threat information.
- For a large number of information sharing elements, no standards or active standardization efforts exist.
- Not many information exchange elements bridge the strategic/policy and tactical levels or the tactical and operational/technical levels.
- Currently, there is a lack of interoperability of standards that would allow the forwarding of information to other stakeholders in a subsequent phase of the incident management cycle. For instance, there is a gap in moving and reusing (technical) detection information to law enforcement.

6. Conclusions

Information sharing of cyber security information is a complex organizational topic as outlined by the good practice document on sharing cyber security information [8]. This chapter has discussed the decomposition of the information sharing domain into a set of information sharing classes and elements using a grid based on the incident management cycle and decision making levels. The mapping shows where information exchange elements fit, the level of decision making they support and the phases of the incident management cycle in which they are involved

The grid of mapped elements facilitates discussions in organizations about the types of information that can be shared with other organizations and the conditions under which the information may be shared. Some information elements can be shared easily while other elements require a base level of trust and a secure means of transfer, processing and storage. For example, the sharp distinction between information exchange elements of strategic importance to organizations and technical intrusion detection data may eliminate internal organizational barriers to information sharing with other public and private organizations.

An organization may decide that the risk of an information security breach is too high to allow the electronic exchange of the information. The information exchange elements help split (i.e., conduct a "triage" of) cyber security information into classes and elements that can be shared without restrictions, that can never be shared, and that can be shared on a case-by-case basis. The grid can also be used to identify the time criticality of elements. The understanding of time criticality of information exchange elements may encourage organizations to fine-tune the triage process before an incident occurs, thereby enhancing organizational preparation for cyber resilience and incident response.

The grid also reveals the lack of standards or standardization efforts for some cyber security information exchange elements. The identified gaps may

be used to develop a roadmap for developing future interoperable standards, especially related to Class A (actors) and Class M (metrics). Moreover, some standardization efforts have overlooked certain needs – these come to the fore in the mappings shown in Figures 1–3 and Table 1. In some cases, only minor changes are required to create a *de facto* standard that provides the required functionality (e.g., merely extending the standard with additional information exchange fields).

Acknowledgement

This research is partly based on the collaborative work of the NATO RTO Research Task Group on Coalition Network Defense Common Operating Picture and on funding from the Dutch Ministry of Security and Justice for research in cross-sector information sharing.

References

[1] L. Beaudoin, M. Gregoire, P. Lagadec, J. Lefebvre, E. Luiijf and J. Tolle, Coalition network defense common operational picture, presented at the *Symposium on Information Assurance and Cyber Defense*, 2010.

[2] R. Bruce, S. Dynes, H. Brechbuhl, B. Brown, E. Goetz, P. Verhoest, E. Luiijf and S. Helmus, International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues, TNO Report 33680, TNO, Delft, The Netherlands; and Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, New Hampshire, 2005.

[3] CIPedia, CIPedia Main Page (`www.cipedia.eu`), 2014.

[4] Council of the European Union, European Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, Brussels, Belgium, 2008.

[5] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 Final, Brussels, Belgium, 2013.

[6] W. Grudzien and W. Semple, WG2 Outcome Draft, European Union Agency for Network and Information Security, Heraklion, Greece (`resilience.enisa.europa.eu/nis-platform/shared-documents/wg2-documents/wg2-outcome-draft/view`), 2013.

[7] E. Luiijf and J. Healey, Organizational structures and considerations, in *National Cyber Security Framework Manual*, A. Klimburg (Ed.), NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, pp. 108–145, 2012.

[8] E. Luiijf and A. Kernkamp, Sharing Cyber Security Information: Good Practices Stemming from the Dutch Public-Private-Partnership Approach, TNO, The Hague, The Netherlands, 2015.

[9] E. Luiijf, M. Klaver, R. Wolthuis and S. van Hooft, Cross-Sector Information Sharing (in Dutch), TNO Report 2014 R10945, TNO, The Hague, The Netherlands, 2014.

[10] Mandiant, OpenIOC: An Open Framework for Sharing Threat Intelligence, Alexandria, Virginia (`www.openioc.org`), 2014.

[11] Ministry of Security and Justice, Cyber Security Assessment Netherlands 2014, The Hague, The Netherlands, 2014.

[12] Multi-State Information Sharing and Analysis Center, Cyber Alert Level Indicator, Center for Internet Security, East Greenbush, New York (`msisac.cisecurity.org/alert-level`), 2014.

[13] National Institute of Standards and Technology, Common Platform Enumeration (CPE) Dictionary, National Vulnerability Database, Gaithersburg, Maryland (`nvd.nist.gov/cpe.cfm`), 2014.

[14] National Institute of Standards and Technology, National Vulnerability Database, Gaithersburg, Maryland (`nvd.nist.gov`), 2014.

[15] P. Pawlinski, P. Jaroszewski, P. Kijewski, L. Siewierski, P. Jacewicz, P. Zielony and R. Zuber, Actionable Information for Security Incident Response, European Union Agency for Network and Information Security, Heraklion, Greece, 2014.

[16] P. Pawlinski, P. Jaroszewski, J. Urbanowicz, P. Jacewicz, P. Zielony, P. Kijewski and K. Gorzelak, Standards and Tools for Exchange and Processing of Actionable Information, European Union Agency for Network and Information Security, Heraklion, Greece, 2014.

[17] SANS Internet Storm Center, InfoCon, SANS Institute, Bethesda, Maryland (`isc.sans.edu/infocon.html`), 2014.

[18] VERIS, VERIS Community Database (`veriscommunity.net/vcdb.html`), 2014.

[19] World Economic Forum, Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience, Cologny/Geneva, Switzerland, 2012.

[20] World Economic Forum, Risk and Responsibility in a Hyperconnected World (WEF Principles), Cologny/Geneva, Switzerland, 2014.

Appendix: Information Sharing Classes and Elements

This appendix contains detailed information about the information sharing classes and elements. It characterizes the classes and elements. Note that the class name abbreviation is derived from the information exchange type. An element with an asterisk is a military cyber security information exchange element that is not described in this chapter. Table 1 outlines the standards and standardization efforts related to specific information exchange elements. In particular, it shows the existing standards (if any) as well as *de facto* standards and other efforts that may partially satisfy the needs of an information exchange element.

Class M: Sharing Cyber Situational Awareness Metrics
Instead of exchanging large amounts of detailed cyber anomaly information to improve collaborative situational awareness, a number of metrics or (aggregation) indicators may be shared to provide a high-level collaborative situational overview.

- **M1 – Cyber alert level:** A single value defines the overall alert level of another organization, denoting whether a significant threat is currently active or whether the other organization is under attack. Examples are the Multi-State Information Sharing and Analysis Center [12] and the SANS Internet Storm Center [17].
- **M2 – Incident summary metrics and statistics:** The number of open incidents that another organization is currently handling and the number of incidents that occurred in the past, including quarterly or yearly aggregates.
- **M3 – Vulnerability assessment metrics:** The number of open vulnerabilities that another organization has identified in total and per type of system (or network) presented in the context of the total number of scanned systems in order to obtain comparable metrics (e.g., average number of open vulnerabilities per host).
- **M4 – Cyber security sensor alert metrics:** The number of intrusion detection system alerts that another organization has received in the form of trend indicators or a top-ten list of intrusion alerts. An absolute number is of less value because it depends on the numbers, types and configurations of sensors and the types of monitored networks.
- **M5 – Risk and impact metrics:** Indicators of the (potential) impact to the mission or business continuity of an organization such as the percentage of automated teller machines affected at a financial institution.

Class I: Sharing Incident Information
Active sharing of cyber incident information enables one collaborating organization to inform the other collaborating organizations about incident observations, detection methodologies and mitigation techniques so that the other organizations may better detect and respond to similar incidents in their infrastructures.

- **I1 – Sharing information about own incident(s):** An organization shares incident information that it has been attacked and that its cyber operational capabilities may be impacted.
- **I2 – Warning a partner organization that it is targeted:** An organization that monitors network traffic may encounter signs of a cyber attack targeting a

partner organization. Sharing such information benefits the potentially affected organization and increases collaborative situational awareness.

- **I3 – Warning a partner organization that it is a cyber attack source:** Warning an organization that it is a source of cyber attacks on other organizations may quickly initiate mitigation actions that are beneficial to all the collaborating organizations.
- **I4 – Sharing cyber actions:** Sharing information about on-going incident response actions and other cyber actions that may impact collaborative business services (missions). Situational reports include on-going actions, mitigation planning, assets affected, estimated time of completion, etc. Hot phase information is highly sensitive and should not be released to the public.
- **I5 – Querying another organization for similar incidents:** An organization queries other organizations for incidents similar to the incident of interest. Useful (sensitive) information may be shared in order to improve the speed and the quality of the (collaborative) incident response.
- **I6* – Tasking order to manage a cyber incident or to take a mitigation action.**
- **I7 – Requesting help to manage a cyber incident:** Another organization with unique capabilities (e.g., knowledge and resources) may be asked to help with the incident response.
- **I8 – Requesting the management of a cyber incident:** Another organization may be asked to manage the cyber incident response.

Class T: Sharing Threat Information
A threat is the potential for compromise, loss or theft of information or supporting cyber services and resources. A threat may be defined by its source, motivation or result; it may be deliberate or accidental, violent or surreptitious, external or internal. Sharing threat information is crucial to achieve and maintain the right cyber defensive posture in collaborating organizations.

- **T1 – Sharing intelligence about threat agents, vectors and consequences:** Sharing intelligence about adversarial cyber threats (source, intent, capability, tactics, techniques, procedures, recent activity, etc.) in order to maximize collaborative cyber defenses (e.g., [10]).
- **T2 – Sharing information on malware analysis:** Malware analysis requires advanced technical capabilities as well as resources that may be available at other organizations. The shared information could include captured malware, signatures, indicators of compromise, analysis techniques, tools and analysis results.
- **T3 – Sharing information on exploit analysis:** Information that allows better detection of a specific threat, effective protection against exploits and information about exploit code availability and its efficiency against various system and network configurations.
- **T4 – Sharing strategic threat information:** This could involve regular strategic level threat analysis and trend prediction [11] or a current situational picture [18].

Class V: Sharing General Vulnerability Information
Vulnerability information is critical to assess an organization's defense posture and to guide the mitigation measures needed to protect against the hostile exploitation of a vulnerability. Inadequate knowledge about a vulnerability exposes networks and systems to hostile exploitation.

- **V1 – Sharing non-public (closed) information about a specific vulnerability:** This involves sharing information within a trusted community.
- **V2 – Sharing public information about a specific vulnerability:** This is accomplished by direct access (e.g., NVD [14]) or by the selective relaying of information by a Computer Emergency Response Team (CERT) or Information Sharing and Analysis Center (ISAC).
- **V3 – Sharing alert and advisory information:** This involves sharing alerts, general advice and background information on a specific vulnerability.

Class D: Sharing Detection and Mitigation Information
Collaborative organizations can mitigate adversary tactics, techniques and procedures by sharing malware and intrusion signatures, patch information, defensive strategies, attack correlation patterns and domain blacklists.

- **D1 – Sharing intrusion signatures:** Sharing intrusion signatures with other collaborating organizations enables all the organizations to enhance their detection capabilities with minimal additional investments. Feedback on the efficiency of signatures could lead to signature refinement.
- **D2 – Sharing patch information:** This involves sharing test procedures, patch efficiency, deployment experiences and information about side effects.
- **D3 – Sharing vulnerability assessment signatures:** Vulnerability scanners allow users to add their custom signatures. Sharing these signatures with other organizations enhances the collaborative resources and may reduce the impact on collaborative services.
- **D4 – Sharing blacklists and whitelists:** Blacklists are lists of suspicious or malicious IP addresses, website URLs and email addresses that can be used to block traffic and detect cyber attacks. Sharing provides collaborating organizations with access to more extensive and up-to-date blacklists. Whitelists provide the reverse filtering capabilities of blacklists.
- **D5 – Sharing malware/exploit file signatures:** Collaborating organizations may share signature patterns of malware or other suspicious files, including file names, patterns, locations, sizes and identifying byte sequences.
- **D6 – Sharing indicator patterns:** An indicator pattern is used to verify that a system or network has been affected by a cyber attack. If the attack cannot be verified, deeper analysis may be required to determine whether a compromise took place.

Class R*: Sharing Dynamic Risk Assessment and Operational Dependencies
Within a military coalition environment, coalition partners may critically rely on shared cyber assets for the successful completion of a mission. Sharing operation dependencies and information about the utilization of certain assets are, therefore,

important. Three elements have been identified: (i) R1 – Sharing assets and operational dependencies; (ii) R2 – Sharing dynamic risk assessment information; and (iii) R3 – Sharing information about cyber events that increase coalition risk.

Class S*: Sharing Information about Coalition-Shared Assets
If coalition partners share (security) health information of shared assets, other coalition partners can make better use of shared assets and react to changes in the health of an asset. Six elements have been identified: (i) S1 – Identifying shared cyber assets; (ii) S2 – Sharing the security status of shared cyber assets; (iii) S3 – Sharing the changes in the criticality of shared cyber assets; (iv) S4 – Sharing the security status of coalition cyber assets; (v) S5 – Sharing security events concerning coalition cyber assets; and (vi) S6 – Sharing risk assessments of coalition mission objectives and cyber assets.

Class C: Sharing Compliance Policies and Status
If an organization knows the compliance requirements and the status of other organizations with which it collaborates to provide an end-to-end service, the cyber defensive posture can be tuned.

- **C1 – Sharing compliance policies:** Strong compliance may correlate with a lower risk of incidents; detection and reaction to certain threats may be faster. Collaboration with a weaker organization requires more security controls at the interface. Sharing compliance information may help organizations fine-tune their security efforts.
- **C2 – Sharing compliance status:** Even if an organization has a strong compliance policy, all its assets may not comply with the security policy. Knowledge of the actual compliance status enables collaborating organizations to tune their security measures. One example is whether or not an organization can be reached 24/7 in order to report a security incident.

Class B: Sharing Background and Reference Information
This category concerns background information that is not directly cyber security information (e.g., contact details and reference information).

- **B1 – Sharing contact information:** This information may include the contact details of the CERT team and the chief information security officer.
- **B2 – Sharing software and hardware product identifiers and characteristics:** This information may include Common Platform Enumeration (CPE) Dictionary data [13].
- **B3 – Sharing network topology information:** Understanding the network structure of another organization may increase the joint cyber situational awareness. Understanding the types of threats and vulnerabilities and the attack paths existing in other organization also improves the joint cyber situational awareness.
- **B4* – Sharing physical locations of sites and mobile platforms:** This helps understand the geolocation-dependent risk of an organization.
- **B5 – Sharing time zone information:** This helps interpret logging and other information pertaining to synchronized attacks against multiple organizations.

Class G: Sharing Good Practices
Similar to sharing threat and incident information, the sharing of product, architecture and configuration information between collaborating organizations can help reduce costs and improve the joint security posture.

- **G1 – Sharing good practice information:** This includes good practice guides, white papers and security architectures.
- **G2 – Sharing security settings:** This includes system configuration information such as the steps required to harden a system.
- **G3 – Sharing recovery procedures and good practices:** This may increase the resilience of cyber services.
- **G4 – Sharing lessons identified:** Sharing information about what was good and what went wrong may help other organizations avoid pitfalls during incident response. This information also increases the level of trust in partner organizations.

Class A: Sharing Actor Information
Multiple organizations, including law enforcement, may need to exchange information about cyber criminal or cyber espionage activities and the actors to be apprehended and potentially prosecuted.

- **A1 – Sharing attribution information:** This includes detailed technical, analytical and sensitive intelligence about attack attribution.
- **A2 – Sharing actor information:** This includes information about the suspected actors.
- **A3 – Sharing lawful interception information:** This involves (electronic) requests to tap certain information flows and to deliver the collected information to law enforcement.
- **A4 – Requesting legal assistance or cooperation:** This involves an (international) request for legal assistance/cooperation to arrest actors, collect and safeguard evidence, and handle notice-and-takedown requests.
- **A5 – Sharing evidence and prosecution information:** This involves sharing information in criminal investigations and for possible prosecution.

Table 1: Information exchange classes and elements.

Class	Standards (see [16])	De facto standards and other efforts
Class M: Sharing Cyber Situational Awareness		
M1: Cyber alert level		MS-ISAC cyber alert level; InfoCon
M2: Incident summary metrics and statistics		Incident statistics [11]; VERIS [18]

Continued on next page

Table 1. Information exchange classes and elements (continued).

Class	**Standards (see [16])**	**De facto standards and other efforts**
M3: Vulnerability assessment metrics		CWSS; CVSS/CCSS
M4: Cyber security sensor alert metrics		No efforts identified
M5: Risk and impact metrics		CWRAF (and CWSS); EBIOS method; Risk management language
Class I: Sharing Incident Information		
I1: Sharing information about own incident(s)	IODEF over RID	IDMEF; VERIS (Commercial)
I2: Warning a partner organization that it is targeted		IODEF (Partial)
I3: Warning a partner organization that it is a cyber attack source	ARF	IODEF (Purpose is mitigation)
I4: Sharing cyber actions	IODEF over RID (Report)	
I5: Querying another organization about similar incidents	IODEF over RID (Query)	VERIS (Commercial)
I6: Tasking order (Military*)		*Military
I7: Requesting help to manage a cyber incident	IODEF over RID (Trace request, Investigation request)	
I8: Requesting the management of a cyber incident		No efforts identified
Class T: Sharing Threat Information		
T1: Sharing intelligence about threat agents, vectors and consequences	STIX over TAXII [16]	OpenIOC; CybOX; CAPEC; NASL
T2: Sharing information on malware analysis	MAEC	OpenIOC; CybOX
T3: Sharing information on exploit analysis		OpenIOC

Continued on next page

Table 1. Information exchange classes and elements (continued).

Class	Standards (see [16])	De facto standards and other efforts
T4: Sharing strategic threat information	SCAP/CAPEC	STIX over TAXII
Class V: Sharing General Vulnerability Information		
V1: Sharing non-public information about a vulnerability	OVAL, CVRF on top of CVE, CWE, ITU-T X.1206; IODEF-SCI/ RFC7203	CWSS; CVSS; CWRAF; DAF Relates to ISO/IEC 29147:2014 and ISO/IEC 30111:2013
V2: Sharing public information about a vulnerability	CVRF, NVD on top of CVE, CWE, ITU-T X.1206	CWSS; CVSS; CWRAF Relates to ISO/IEC 29147:2014 and ISO/IEC 30111:2013
V3: Sharing alert and advisory information		CAP; CVRF; CAIF (Simple factsheets)
Class D: Sharing Detection and Mitigation Information		
D1: Sharing intrusion signatures	OpenIOC	OVAL; XCCDF
D2: Sharing patch information	OVAL; ITU-T X.1206	ISA-TR 62443-2-3 (Draft)
D3: Sharing vulnerability assessment signatures	OVAL; XCCDF	NASL
D4: Sharing blacklists and whitelists		Blacklists and whitelists (ASCII)
D5: Sharing malware/exploit file signatures		OpenIOC
D6: Sharing indicator patterns	CybOX; MEAC	OpenIOC; NASL
Class B: Sharing Background and Reference Information		
B1: Sharing contact information	SCAP	AI

Continued on next page

Table 1. Information exchange classes and elements (continued).

Class	**Standards (see [16])**	**De facto standards and other efforts**
B2: Sharing hardware and software product identifiers and characteristics	SCAP/CPE	AI; CPE; CCE; SACM (Draft)
B3: Sharing network topology information		AI; CCE; SACM (Draft)
B4*: Sharing physical locations of sites and mobile platforms		*Military (Possible civilian use)
B5: Sharing time zone information		No efforts identified
Class C: Sharing Compliance Policies and Status		
C1: Sharing compliance policies		No efforts identified
C2: Sharing compliance status		PLARR (ASR/ARF); XCCDF; XDAS
Class G: Sharing Good Practices		
G1: Sharing good practice information		CVRF (Mitigation)
G2: Sharing security settings		OVAL; XCCDF; PLARR (ASR/ARF); CCE
G3: Sharing recovery procedures and good practices		No efforts identified
G4: Sharing lessons identified		No efforts identified
Class A: Sharing Actor Information		
A1: Sharing attribution information		STIX over TAXII; CDESF (Terminated)
A2: Sharing actor information		STIX over TAXII
A3: Sharing lawful interception information	RFC 3924; TIIT (Transport of intercepted traffic)	ETSI lawful intercept standards

Continued on next page

Table 1. Information exchange classes and elements (continued).

Class	**Standards (see [16])**	**De facto standards and other efforts**
A4: Requesting legal assistance or cooperation		No efforts identified
A5: Sharing evidence and prosecution information		STIX over TAXII (Incomplete)
Class S*: Sharing Information about Shared Cyber Assets		
S1*: Identifying shared cyber assets		*Military
S2*: Sharing the security status of shared cyber assets		*Military
S3*: Sharing changes in the criticality of shared cyber assets		*Military
S4*: Sharing the security status of coalition cyber assets		*Military
S5*: Sharing security events concerning coalition cyber assets		*Military
S6*: Sharing risk assessments of coalition mission objectives and cyber assets		*Military
Class R*: Sharing Dynamic Risk Assessment and Operational Dependencies		
R1*: Sharing assets and operational dependencies		*Military
R2*: Sharing dynamic risk assessment information		*Military
R3*: Sharing information about cyber events that increase coalition risk		*Military