CYBER INCIDENT CLASSIFICATION

A Report on Emerging Practices within the OSCE region

OSCE
Organization for Security and
Co-operation in Europe

Published by the Organization for Security and Co-operation in Europe
Vienna, November 2022

Layout and design by Peno Mishoyan

ISBN 978-92-9271-044-6
Transnational Threats Department
OSCE Secretariat
Wallnerstrasse 6, A-1010 Vienna, Austria
https://www.osce.org/secretariat/cyber-ict-security

The publication of this report was made possible thanks to generous contributions from the Federal Republic of Germany and French Republic. The content of this publication, including the views, opinions, findings, interpretations and conclusions expressed herein do not necessarily reflect those of these donors. It is not a consensus-based document.

This publication is published in line with the mandate of the OSCE Transnational Threats Department. The OSCE Secretariat does not accept any liability for the accuracy or completeness of any information, for instructions or advice provided, or for misprints. The OSCE Secretariat may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Organization for Security and
Co-operation in Europe

Contents

Acknowledgments

This report was prepared by the OSCE Transnational Threats Department (TNTD) Co-ordination Cell under the direction of Ms. Szilvia Tóth, Cyber Security Officer. TNTD would like to thank Dr. Camino Kavanagh for her research and for preparing the report. Valuable support was provided by Ms. Ružica Stojičić Bencun of TNTD Co-ordination Cell.

List of Acronyms and Abbreviations

CBM	Confidence-Building Measure
CERT	Computer Emergency Response Team
CIT	Cybersecurity Incident Taxonomy
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Cybersecurity
EU	European Union
FIRST	Forum of Incident Response and Security Teams
ICT	Information and Communications Technology
NCICS	National Cyber Incident Classification System
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OSCE	Organization for Security and Co-operation in Europe
UN	United Nations
US	The United States of America

Foreword

The OSCE is the world's largest regional security organization, encompassing 57 participating States in Europe, Asia and North America. The Organization's cross-dimensional approach to security lent itself to efforts in disarmament and implementation of security- and confidence-building measures in a number of security areas. In cyber/ICT security, participating States quickly recognized a potential for applying confidence-building measures (CBMs) in cyberspace. The OSCE plays a pioneering role in enhancing cyber/ICT security, being the first regional organization to develop CBMs to reduce the risks of conflict stemming from the use of ICTs among its participating States.

In the past decade, regional organizations have served as incubators of UN recommendations on international ICT security. This momentum was recently reinforced by landmark reports adopted by the UN Open-Ended Working Group on "developments in the field of information and telecommunications in the context of international security" and by UN Group of Governmental Experts on "Advancing responsible State behaviour in cyberspace in the context of international security". Both reports recognize the importance of regional and sub-regional organizations in developing and implementing CBMs in their respective regions.

Since 2013, OSCE participating States have adopted and continue to work on the implementation of 16 cyber/ICT CBMs, due to the fact that the CBM process is practical, voluntary and depoliticized in nature. As such, it has proven its worth as a tool to strengthen inter-State collaboration, create transparency, and foster greater preparedness. The OSCE Secretariat's Transnational Threats Department supports participating States in the implementation of cyber/ICT security CBMs, by providing a platform to conceptualize and exchange best practices on such topics as public-private partnerships, responsible reporting of vulnerabilities and critical infrastructure protection.

The foundation for this report is in CBM 15, through which participating States agreed to —on a voluntary basis—*"encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies"*. One of the areas of collaboration is the adoption of voluntary national arrangements to classify ICT incidents by their scale and seriousness.

The report highlights emerging practices in national classification of cyber incidents by underlining commonalities in existing approaches to cyber incident classification among OSCE participating States and identifying limitations in this process. Although experiences in developing cyber incident classification systems are diverse across participating States, the knowledge derived from these processes could be used as a capacity-building tool to promote the use of national cyber incidents classification systems within the OSCE area and beyond.

Alena Kupchyna
Co-ordinator of Activities to Address Transnational Threats
OSCE Secretariat

Executive Summary

In January 2022, the Secretariat of the Organization for Security and Co-operation in Europe (OSCE), in the framework of an extra-budgetary project, embarked on a study of emerging practices in cyber/ICT incident classification in the OSCE region. To inform this study, it disseminated a questionnaire to OSCE participating States. An analysis of the survey results along with a review of publicly available documents referenced in participating States' responses suggest that greater attention is being paid to cyber incident classification across the region and that these systems are viewed as critical to managing cyber incidents at the national level and for engaging with other States on cyber incidents at the regional and international levels.

A growing number of OSCE participating States already have, or are in the process of establishing a national cyber/ICT incident classification system. Many have also established or are reviewing the policy and legal basis for cyber incident classification or are moving in that direction. In several States, their system is closely tied to national plans for crisis management or emergency planning. Responsibility for the development and co-ordination of NCICS varies across the region. Existing practices confirm that, for incident classification to be effective, co-operation between a broad range of public and private actors and sectors, including, for instance, government agencies, CERTs[1]/CSIRTs[2] or similar, operators of essential services and digital service providers, is necessary. The importance of engaging relevant non-State actors such as cyber security researchers is increasingly acknowledged by some participating States.

The study also provides insights into some of the challenges OSCE participating States are facing in developing and implementing their cyber incident classification systems. These challenges range from personnel and resource constraints, to agreeing on a common classification taxonomy that is clearly communicated to and used by all intended constituencies, but also interagency co-operation and information sharing as well as reviewing and adapting the system once in place. The study suggests that efforts are underway to overcome many of these challenges and that capacity building and other forms of co-operation will play an important role to that end. Several participating States have voiced an interest in availing of the OSCE to exchange national experiences on incident classification and to potentially engage in more dedicated exchanges on the topic, including crisis management exercises.

The study also suggests that these emerging practices and related challenges, which are presented below under the rubrics **purpose**, **policy**, **process** and **people**, be taken up within further exchanges among OSCE participating States and between the OSCE and other regions. These discussions would ensure further advancements in the spirit and intent of the OSCE cyber/ICT CBMs, particularly CBMs 15 and 3[3], as well as those agreed at the UN.

[1] CERTs—Computer Emergency Response Teams
[2] CSIRTs—Computer Security Incident Response Teams
[3] Permanent Council Decision No. 1202 | OSCE

P PURPOSE AND OBJECTIVES

Clarity about the purpose and objectives of the cyber incident classification system and its core stakeholders and constituents is a critical first step in its implementation and socialisation.

P POLICY AND LEGAL BASES

Having a sound policy and/or legal base for cyber incident classification is critical to ensuring its effectiveness as well as its sustainability. Clear provisions on overall responsibility for the system, interagency co-operation, reporting and notification, data-handling procedures, resource allocation and review procedures are equally important. Furthermore, ensuring appropriate linkages with broader national crisis/emergency management policy or legislation is also essential.

In a national context, it is important to have clearly articulated guidance in place, which specifies:

- The policy and legal base for what the cyber incident classification is setting out to achieve;
- Who co-ordinates its development and implementation;
- Who its key stakeholders/constituencies are;
- What the process of categorizing and prioritizing an incident entails;
- The response mechanisms for incidents;
- What would happen to activate a specific classification; and
- How regularly the incident classification system is reviewed and what the review process entails.

The process of developing a cyber incident classification can be lengthy and resource intensive as well as challenging, especially in its initial phases.

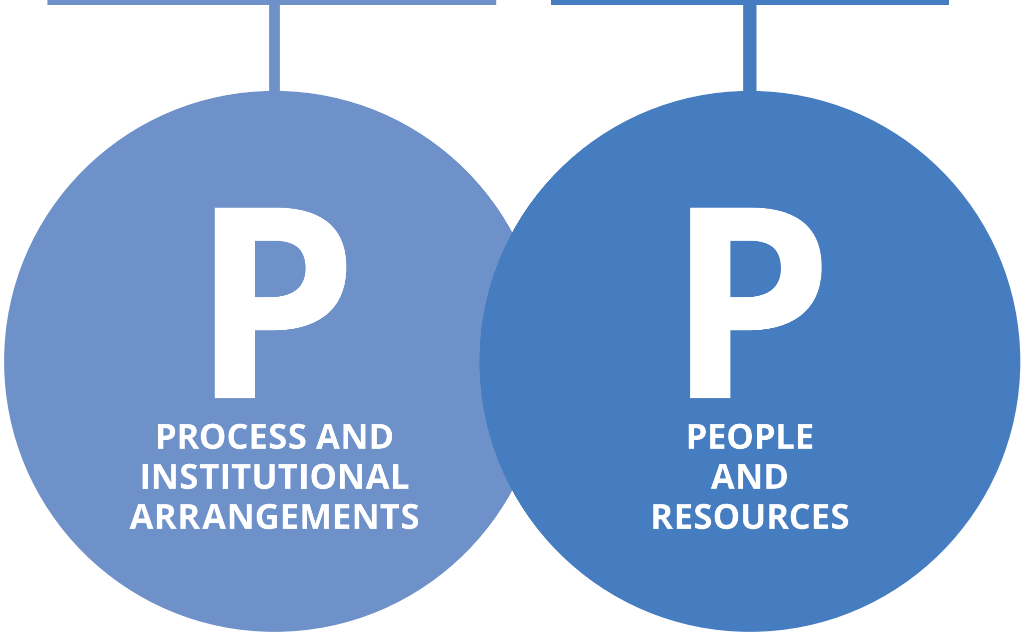
A standard approach to categorizing and prioritizing cyber incidents in accordance with their severity and scale is important for diagnosing an incident and relating the importance of the incident to its impact on a specific institution, entity or sector and its urgency, relative to the timing of the incident.

Once established, a cyber incident classification system should be regularly reviewed to assess its effectiveness and ensure it is appropriately informing a country's incident response and its risk or emergency management posture.

Sharing national approaches to classifying ICT incidents in terms of the scale and seriousness of the incident with other States can contribute to building confidence between States and help avoid potential misunderstandings that may emerge around cyber incidents and related response measures, thus contributing to regional and international security and stability.

The expertise/skills/capacity required to design, manage and sustain a cyber incident classification system is multi-faceted and involves a range of expertise and responsibilities.

These skills need to be appropriately budgeted for and core duties adequately considered in the planning processes.



P

PROCESS AND INSTITUTIONAL ARRANGEMENTS

P

PEOPLE AND RESOURCES

Chapter 1

Background and Introduction

In 2021, the OSCE initiated an extra-budgetary project focused on CBM 3 and CBM 15, specifically on cyber/ICT crisis communication procedures, crisis management and the classification of ICT incidents in terms of the scale and seriousness of the incident. The project aims to raise the implementation rate of the OSCE cyber/ICT CBMs, as well as enhance capacities of OSCE participating States to deal with significant cyber/ICT incidents in an effective way through providing support in developing national cyber incident severity scales.

Recognizing the increasing complexity of cyber/ICT security incidents and the need for advancing crisis management procedures and expanding the classification of cyber/ICT incidents in terms of their scale and seriousness, the OSCE Secretariat's Transnational Threats Department aims to promote, assist and foster the use of national cyber incident severity scales in OSCE participating States through the aforementioned extra-budgetary project. Rather than only focusing on severity scales per se, the project is taking a broader approach to cover the processes, capacities, resources and institutional arrangements required to design, develop and implement such scales, hence the reference throughout the document to national cyber incident classification systems.

Drawing from CBM 15 on critical infrastructure protection and CBM 3 on consultation procedures in particular, the project acknowledges that creating a cyber/ICT incident classification system can contribute significantly to enabling the proper prioritization and management of incidents, particularly those affecting critical infrastructure at both the national and regional levels.

In January 2022, the OSCE commenced a study aimed at analysing emerging practices in cyber incident classification amongst OSCE participating States and identifying the interests and needs of participating States in this area. The study draws from the results of two surveys and documentation provided by participating States. In addition to serving as important input for further exchanges between participating States on the topic, the report highlights a range of approaches and practices that can serve as guidance for States and other relevant stakeholders on cyber incident classification.

Links to publicly available documents provided by respondents have been included in the annex to the report.

Chapter 2

Cyber Incident Classification in the OSCE Region

2.1 Purpose of a national cyber incident classification system

This section of the report explores questions faced when establishing cyber incident classification systems, including whether such a system is already in place and if not, whether there are plans underway to establish such a system. Importantly, it considers views on the purpose of such systems and explores whether existing approaches derive from or are tied to broader policy and legislative frameworks. It also delves into the question of roles and responsibilities relevant to cyber incident classification systems, including co-ordination of the development and implementation of the classification system and those entities that might be involved in the process of classifying cyber incidents.

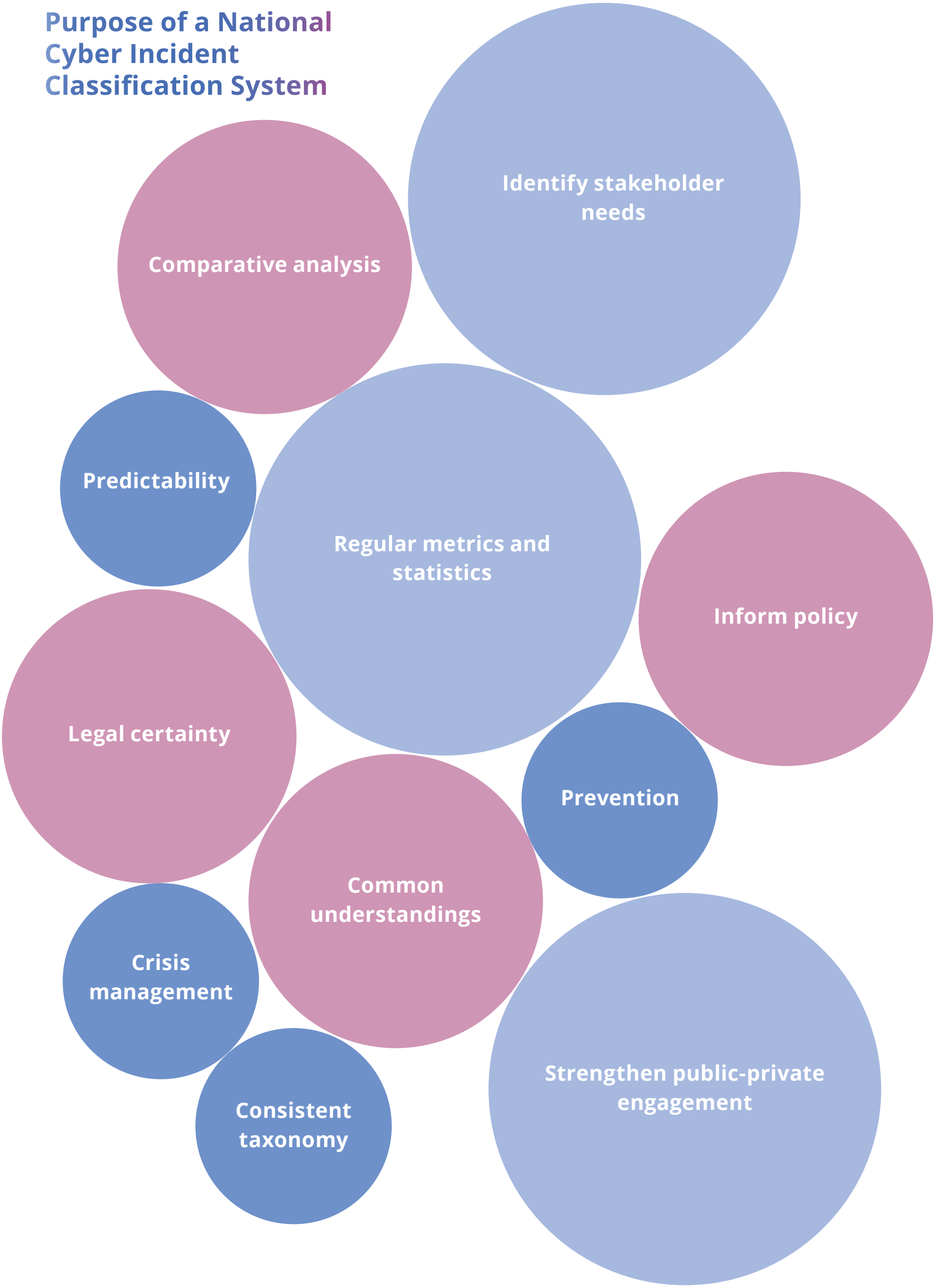
OSCE participating States have taken different approaches to cyber incident classification. While some systems have been in place over two decades, most were established after 2015. Many of these classification systems and enabling legislative or regulatory instruments are publicly available online. Some countries that do not currently have a cyber incident classification system in place plan to establish one within the next two years.

In general terms, the purpose of a NCICS is to generate a clear picture of the cyber threat landscape, to ensure a prompt response to cyber/ICT incidents and to minimise the damage they can cause. More specifically, it is a means to support national crisis management and incident response processes by providing a routine and consistent mechanism that can be used to objectively assess and prioritize cyber incidents in the national context, in a timely manner, and to identify gaps in existing defences. Such a mechanism in turn informs decision-making - including at strategic and political levels - relevant to the nature and timeliness of the response and the procedures for moving from identification of an incident to its treatment and eventual resolution, while minimising disruption to network operations. It is important that the purpose of a cyber incident classification and its core stakeholders and constituents is clearly articulated from the outset.

Importantly, a cyber incident classification system also informs decision-making relevant to who leads or co-ordinates each step of the response, as well as to effort and resource allocation or requirements. In some instances, it may be accompanied by an entity responsible for managing incidents.

In addition, a NCICS can help develop shared situational awareness of cyber incidents and make comparisons with peers, including through more routine exchanges of information across organizations. It can also help ensure consistency and clarity in the way an incident is communicated within and across organizations, or to the broader public.

Purpose of a National Cyber Incident Classification System



Identify stakeholder needs

Comparative analysis

Predictability

Regular metrics and statistics

Inform policy

Legal certainty

Prevention

Common understandings

Crisis management

Consistent taxonomy

Strengthen public-private engagement

RECOMMENDATION 1

The purpose of a NCICS is to generate a clear picture of the cyber threat landscape and ensure a prompt response to cyber/ICT incidents and minimize the damage they cause.

A NCICS supports national crisis management by providing a routine and consistent mechanism to objectively assess the risk of a cyber incident in the national context, in a timely manner, and detect possible gaps in existing defences.

Nationally a cyber incident classification system can contribute to:

- reaching common understanding of what is (and what is not) a cyber incident.
- ensuring more consistency in cyber incident terminology or lexicon (taxonomy) across organizations and constituents nationally, and in information exchanges with other countries.
- determining retroactively if the assessment was correct, and track changes over time.
- ensuring greater alignment and consistency between different national-level crisis management tools or plans (e.g., between national cyber emergency plans and national emergency management plans).
- identifying the needs of different stakeholders and constituencies and how the classification system can be adapted to those needs.
- developing regular metrics, statistics and comparative analysis to inform more consistent threat landscaping or projections and to inform forward planning.
- preventing future incidents from occurring.
- informing policy and regulatory development, especially regarding monitoring and reporting requirements relevant to high-risk incidents.

- providing greater legal certainty [or greater predictability] for organizations and relevant stakeholders.

Internationally a classification system can also serve as a basis for or contribute to:

- facilitating exchanges of information between different states or services across the region on their approaches to incident classification (including on what a cyber incident can be and how governments should deal with it), which in turn can strengthen confidence and co-operation and reinforce mutual understandings.
- assessing and comparing statistics with other countries.

RELATION WITH BROADER NATIONAL CYBER INCIDENT OR CRISIS MANAGEMENT FRAMEWORK AND NATIONAL LEGISLATION

RECOMMENDATION 2

Cyber incident classification systems are generally anchored in national policy and other relevant frameworks and often flow from or are anchored in national legislation.

Cyber incident classification systems are generally anchored in national policy or other relevant frameworks (e.g., national information security, cyber security or cyber incident systems or frameworks; national cyber emergency plans; cyber security event management plans).

However, the place of a cyber incident classification system in any given country's national incident or crisis management policy hierarchy may depend on the level of a given incident (or set of incidents) or how high it is scored in relation to its relevance to national security. In some cases, only certain elements of a plan may be made public. For instance, a government may have a public cyber/ICT security event management plan, while the national centre for cyber/ICT security may have a separate, non-public plan accessible only to the centre.

Often, the cyber incident classification system flows from or is anchored in national legislation (e.g., in an information or cyber security act; a law on cyber or information security; a federal law on the safety of critical information infrastructure). It may also be included in legislation outlining the functions of incident or emergency response teams (CERTS or CSIRTs), in regulatory instruments (e.g., on the cybersecurity of operators of essential services and digital service providers) or incident-specific regulation (e.g., on incident notification); or in decrees, orders or presidential authorities. In the case of members of the EU, their classification systems draw directly from the Network and Information Systems (NIS) Directive[4] and in future will likely be more closely integrated into general national crisis management frameworks.[5] Cyber incident classification may also be relevant to or included in other pieces of crisis management legislation or policy (e.g., a civil protection act) as a means to support a wider diffusion and use of the tool.

RECOMMENDATION 3

A sound policy and/or legal base for cyber incident classification is critical to ensuring its effectiveness as well as its sustainability.

Introducing clear provisions on overall responsibility for the system, interagency co-operation, reporting and notification requirements and procedures, data-handling procedures, resource allocation and review procedures are equally important.

In some cases, the cyber incident classification system was preceded by other legislation, policies, strategies or plans relevant to cyber or information security, cyber defence, the security of information technologies or incident management, reflecting an incremental

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[5] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148, Doc. No. 14337/21, 26 November 2021, Art. 7, para. 3 (b) on cybersecurity crisis management procedures.

process leading to the system or approach currently in place. In other cases, classification systems emerged organically early on, in response to the growing severity of cyber incidents. In the case of the EU, these existing systems or approaches have continued to mature, gradually aligning with or integrating elements of the NIS Directive's cyber incident taxonomy, which, in many cases, was or is being developed by national CERTs or CSIRTs. These, in turn, often use playbooks for incident classification, which tend to be very detailed, specific to the organization and very dynamic.

SCOPE OF NATIONAL CYBER INCIDENT CLASSIFICATION SYSTEMS

A key step in the process of developing a national cyber incident classification system is clearly identifying its scope, i.e., its main stakeholders or constituencies. This entails establishing criteria for assessing the risk profiles of different stakeholders and constituents in terms of how critical they are to the functioning of society and the economy, which, in turn, requires accommodating very diverse public and private interests, ranging from government bodies to critical infrastructure assets or services, to businesses (small, medium and large), communities and individuals. It is equally important that the system be flexible enough to accommodate additional stakeholders/constituents as the threat landscape changes in tandem with our dependency on ICTs.

RECOMMENDATION 4

Establishing clear criteria to determine the stakeholders or constituencies that a national cyber incident classification will serve, including how critical they are to society and economy requires serious consideration. The approach should be flexible enough to accommodate new stakeholders and constituents as the threat landscape changes.

In the OSCE region, to date, the main stakeholders/constituencies of national incident classification systems include a range of government agencies (e.g., offices of the head of government, ministries of the interior/homeland security, justice, defence, foreign affairs, economic affairs and digital transformation; national intelligence agencies, departments or bureaux; and national cyber or information security agencies or entities), 'essential' or 'important' sectors or services deemed critical to the functioning of society or the economy, critical infrastructure asset owners, businesses, and individuals.

REQUIREMENTS (E.G., GOVERNMENT-MANDATED REPORTING OR NOTIFICATION REQUIREMENTS) STEMMING FROM NATIONAL CYBER INCIDENT CLASSIFICATION SYSTEMS

Uniform and consistent reporting on incidents is critical to the effectiveness of cyber incident classification systems.

Often, reporting and/or notification requirements stem from the NCICS. The requirements vary, with some stemming from national cyber/ICT security- or incident-related legislation or policy frameworks that provide for a variety of government actions.

RECOMMENDATION 5

Uniform and consistent reporting on incidents is critical to the effectiveness of cyber incident classification systems and helps determine the nature of the response.

In some jurisdictions and depending on the severity of an incident and the entity affected, incident reporting is legally required.

Reporting or notification requirements tend to be linked to incidents that are categorized higher up in the severity scale in accordance with a given country's scoring system, which as discussed earlier, can be presented in a variety of ways (colour scheme, numerical ratings, range of severity etc.) and depends on the entities affected (e.g., operators of essential services; digital service providers; government entities; critical infrastructure sectors; information infrastructure operators) and the continuity of their services; the number of people affected (e.g., if an incident (could) affect more than 500,000 people) etc.

While mid- or lower-level incidents do not necessarily trigger reporting or notification requirements, in some instances reporting or notification may be accepted or recommended. For instance, a National Cyber Incident Response Plan may still recommend reporting minor incidents as a means to achieve wider situational awareness.

For the EU, operators of essential services and digital service providers are required to notify the relevant competent body (e.g., national cyber or information security agency; CSIRT/CERT; security incident response institution) in the case of security incidents that have significantly impacted the continuity of the essential or digital services they provide. Detailed instructions in this regard outline the time frame; means of notification; and information that should be provided to the competent body upon notification of the incident. The competent body is in turn responsible for reporting the incident up the policy ladder to the political level where a decision is made on whether to activate crisis management mechanisms. How a cyber incident is classified will generally dictate factors such as who leads the response, and the support arrangements that will be mobilised accordingly.

GUIDANCE TO SUPPORT IMPLEMENTATION OF INCIDENT CLASSIFICATION FRAMEWORKS

Guidance development is a process that is critical to the implementation of policy. Engaging relevant stakeholders during the guidance development process can improve guideline recommendation uptake. Where cyber incident classification is concerned, in a national context, it is important to have in place clear guidance that specifies inter alia, the policy and legal base for what the cyber incident classification is setting out to achieve; who co-ordinates its development and implementation; who its key stakeholders/constituencies are; what the process of categorizing and prioritizing an incident entails; and how regularly the incident classification system is reviewed and what the review process entails.

Where OSCE practice is concerned, only a few participating States have developed guidance to accompany implementation of their classification system. For those that have, such guidance is embedded in, or draws from, regional (e.g., EU) or national policy, legislation, standards, or regulation relevant to cyber incident or broader emergency planning and can also link to other types of incident response-related guidance (e.g., guidance on observed activity, identified threats etc.) In some cases, guidance is broad enough to be nation-wide and applicable to any sector and/or enterprise, while in others it is sector (e.g., for the financial sector) or enterprise specific.

RECOMMENDATION 6

Clearly articulated guidance contributes to the effective implementation and socialization of a cyber incident classification system. Such guidance can specify: the purpose of the cyber incident classification system and its policy and/or legal basis; who co-ordinates its development and implementation; its scope/coverage in terms of its key stakeholders/constituencies; definitions and explanations of categories and priorities; the response mechanisms for incidents, including an explanation of what would activate a specific classification, which organization responds and what actions they would take; and how regularly the incident classification system is reviewed and what the review process entails.

Examples of existing guidance include:

- US NCCIC Scoring System (nation-wide sector guidance on implementation of the scoring system), which is based on the NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide, and tailored to include entity-specific potential impact categories that allow NCCIC personnel to evaluate risk severity and incident priority from a nationwide perspective.

- For members of the EU, relevant guidance can be. found in the NIS Directive and national sectorial regulations.
- The French severity scale to classify cyberattacks was developed within the framework of the strategic review of cyber defense published in 2018. Incorporating national and international legal standards, it is built both as a decision-making tool for authorities and a support for international co-operation.

2.2 Process and Institutional Arrangements

This section of the report highlights the capacities and resources that might be required to develop, manage and sustain a national cyber incident classification system, as well as related processes and arrangements. It explores approaches to classifying cyber incidents, what existing systems set out to measure, whether specific schemas are used, how they are presented and defined/explained, and the criteria that are considered when an incident is being classified in terms of severity/ seriousness. It also discusses review procedures, and explores whether specific requirements stem from the system. It concludes with an essential discussion on some of the core challenges States have encountered when developing and implementing national cyber incident classification systems.

INSTITUTIONAL RESPONSIBILITIES: THE NATIONAL ENTITIES RESPONSIBLE FOR DESIGNING AND CO-ORDINATING DECISIONS ON CYBER INCIDENT CLASSIFICATION

RECOMMENDATION 7

Cyber incident classification is generally a centralized process co-ordinated by a central entity or authority and involving a range of government bodies. Depending on the context, ***it may also include essential or important*** *services/critical infrastructure asset owners or operators, digital service providers and other private sector entities.*

Responsibility for the development and co-ordination of national cyber incident classification systems varies significantly. In some cases, this role is held by a central co-ordinating entity (e.g., a national security council under which a national cyber security council is; an interagency co-ordination body; a national computer incident response and co-ordination centre).

In other instances, the responsibility is held by a dedicated cyber or information security entity or authority (e.g., national cyber or information security agency; national cyber security directorate; information systems security bureau; government information security office; national authority for electronic certification and cyber security; e-government state agency).

In some cases, a specific ministry plays this role, while in others, it is the role of a national CERT or CSIRT, sometimes with specific reporting requirements in the case of serious incidents (e.g., to a national police commission). Engaging of relevant stakeholders and constituencies in the design and development of the classification system can contribute to building trust between public and private actors and within and across sectors and services from the outset.

NATIONAL APPROACHES TO CYBER INCIDENT CATEGORIZATION AND PRIORITIZATION

A standard approach to categorizing and prioritizing cyber incidents in accordance with their severity and scale is important for diagnosing an incident and relating the importance of the incident to its impact on a specific institution, entity or sector and its urgency, relative to the timing of the incident.

Categorization speeds up the process of incident classification and creates greater efficiency within the process flow while priority assignment can help ensure a common lexicon when an incident is being discussed, help determine urgency, incident response and reporting requirements, as well as recommendations for leadership engagement.

Incident priority designation can help ensure a common lexicon when an incident is being discussed. It also helps determine urgency, incident response and reporting requirements, as well as recommendations for leadership engagement.

Using a standard methodology to categorizing and prioritizing cyber incidents seems to be the common approach, in some cases anchored in national legislation (e.g., in a cyber or information security act, a royal decree), with more detail provided in national plans (e.g., a national cyber incident response plan, a cyber defense review) which define unified processes for categorizing and reporting different types of incidents.

Statutory notification requirements can also provide more detail, with each requirement including a defined set of incident categories.

RECOMMENDATION 8

A standard approach to categorizing and prioritizing cyber incidents in accordance with their severity and scale is important for diagnosing an incident and relating the importance of the incident to its impact on a specific institution, entity or sector and its urgency, relative to the timing of the incident.

Categorization speeds up the process of incident classification and creates greater efficiency within the process flow while priority assignment can help ensure a common lexicon when an incident is being discussed, help determine urgency, incident response and reporting requirements, as well as recommendations for leadership engagement.

Incident priority designation can help ensure a common lexicon when an incident is being discussed. It also helps determine urgency, incident response and reporting requirements, as well as recommendations for leadership engagement.

Based on the material reviewed for this study, some States first categorize a cyber incident and then assign it priority, while some only attend to the first. Ideally, both should be covered.

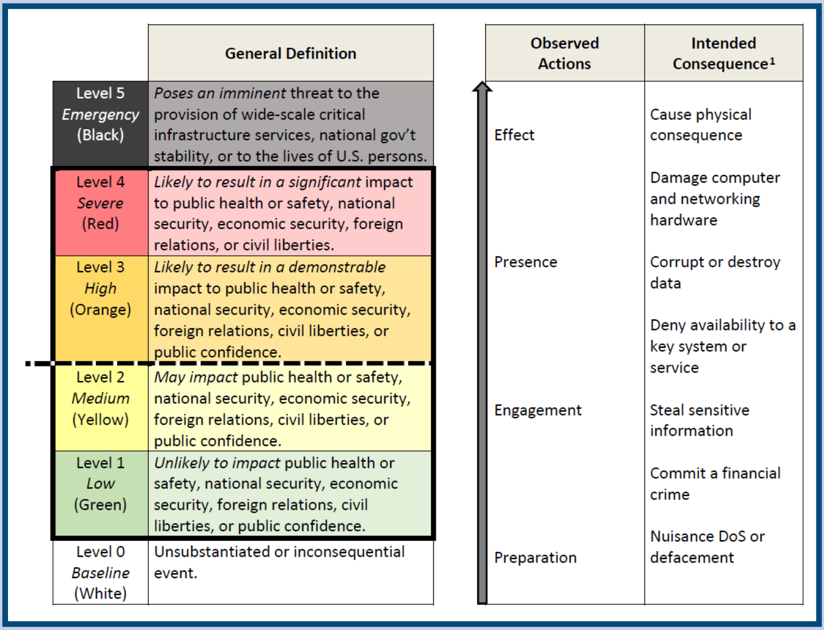
Other taxonomies developed by private entities can also be useful to consider when developing NCICS.[6]

[6] See, for example, FIRST Metrics SIG; FIRST DNS Abuse SIG; the MITRE framework.

EXAMPLES

THE US APPROACH

The US approach to incident categorization involves a scoring system based on eight different categories of incidents: Functional Impact; Observed Activity; Location of Observed Activity; Actor Characterization; Information Impact; Recoverability; Cross-Sector Dependency; and Potential Impact. A weighted arithmetic mean is used to arrive at a score between zero and 100. Each category is assigned a weight and the response to each category has an associated score. Each response score is then multiplied by the category weight, and the weighted scores are added together. Once the score is determined, the incident is then assigned a priority for which a colour scheme is used, with priorities ranging from Baseline (baseline minor (blue) and baseline negligible (white)) to Low (green) all the way up the ladder to Emergency (black). In addition, the schema also assesses whether incidents are connected and how incident aggregation should be considered when assessing a campaign.



	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

Source: https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf (pg 38)

FRANCE'S SYSTEM

France uses a similar system although it includes a comparison of its criteria to those used in the US system, has set criteria for impact (ranging from negligible to extreme) and assesses the incident against whether it constitutes an armed attack as per Article 51 of the UN Charter. A colour (white to red) and numbering (0-5) scheme is used to assign priority to the incident.

GRAVITY SCALE	EQUIVALENCE WITH THE US CISS	IMPACTS	CHARACTERIZATION AS ARMED AGGRESSION WITHIN THE MEANING OF ARTICLE 51 OF THE UNITED NATIONS
LEVEL 5 - EXTREME EMERGENCY	Level 5 Emergency (Black)	Extreme Impact	Probably possible: to be considered on a case by case basis.
LEVEL 4 - MAJOR CRISIS	Level 4 Severe (Red)	Major Impact	
LEVEL 3 - CRISIS	Level 3 High (Orange)	Strong and Extensive Impact	Probably not possible: actions corresponding to these levels could nonetheless constitute other internationally wrongful acts (intervention, violation of sovereignty, use of force, etc.).
LEVEL 2 - SERIOUS INCIDENT	Level 2 Medium (Yellow)	Strong and circumscribed impact	
LEVEL 1B - INCIDENT	Level 1 Low (Green)	Medium and circumscribed impact	
LEVEL 1A - SIGNIFICANT EVENT		Low impact	
LEVEL 0 - EVENT	Level 0 Baseline (White)	Negligible Impact	

Source: http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

CYBERSECURITY INCIDENT TAXONOMY'S SYSTEM

In some cases, the incident classification system is often based on the CIT, developed by the NIS Cooperation Group.[7] The approach is structured around the nature of the incident (i.e., the underlying cause that triggered the incident); severity of the incident (from low to high); impact of the incident (i.e., the affected services, sectors); the scale of the impact nationally, for economy and society

[7] European Union, Cybersecurity Incident Taxonomy, NIS Cooperation Group, CG Publication 04/2018 https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

(using a colour schema from white to red); and outlook (i.e., the prognosis of the impact (from improving to worsening). Some also use the ENISA[8] Reference Incident Classification Taxonomy (which also informed the NIS CIT) as a starting point for incident classification. It is centered on ten incident types (abusive content, malicious code, information gathering, intrusion attempts, intrusion, availability, information content security, fraud, vulnerable, and other). Many European CSIRTs or relevant bodies already use this taxonomy, often in conjunction with an incident 'category' scale based on incident severity.

CONCLUSION

Learning from other States and drawing from their experiences is also important. In this regard, one participating State noted that its classification matrix (severity and impact presented on an axis) was influenced by the cyber incident categorization system developed by the National Cyber Security Centre (NCSC) of the United Kingdom.[9] Said system includes 6 categories, with category 1 representing a national emergency. Like others, it also includes category definitions, as well as explanations of who responds, and what that response entails across each category.

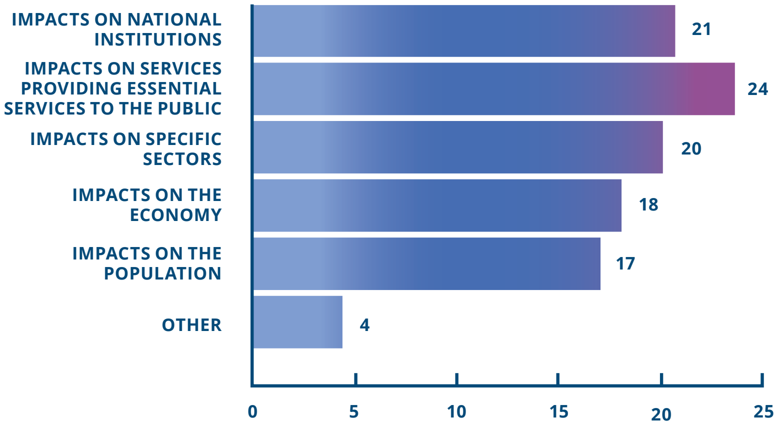
[8] ENISA - The European Union Agency for Cybersecurity - Reference Incident Classification Taxonomy https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/

[9] The UK National Cyber Security Centre's updated incident categoriation system is available here: https://www.ncsc.gov.uk/pdfs/news/new-cyber-attack-categorization-system-improve-uk-response-incidents.pdf

COMMONALITIES IN CATEGORIZING AND PRIORITIZING CYBER INCIDENTS

In accordance with existing approaches, when categorizing incident types, participating States generally assess the *impact of a cyber incident* on the following:

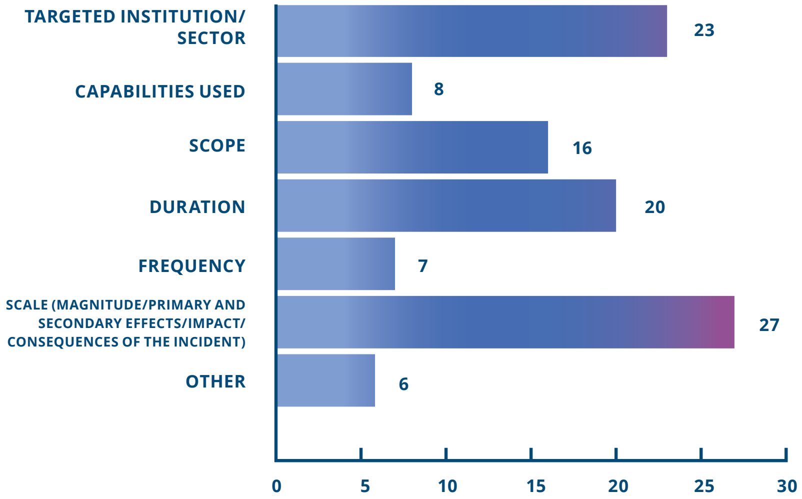
Impacts the Classification System is Aiming to Measure



There are also many commonalities regarding the criteria for classifying an incident in terms of its severity and/or seriousness. These criteria include: scale (magnitude/primary and secondary effects/impact/consequences of the incident), targeted institution/sector, duration, scope, capabilities used, frequency and other.

Mostly two or more of the listed criteria are used, with *scale*, *targeted institution*, *duration* and *scope* being the most commonly cited, followed by *capabilities used* and *frequency*.

What key criteria are considered when an incident (or series of incidents) is being classified in terms of severity and seriousness?



Once an incident is scored or assessed, the next step is to assign it priority. Priority assignments contribute to ensuring common lexicon when an incident is being discussed. They help determine urgency, incident response, reporting requirements, as well as recommendations for leadership engagement.

Options for priority level designation include:

1. Low-critical
2. Levels 1-5
3. Colour schema

Ideally, the priority assignation would include an explanation or definition of each level. For instance, the colour black may represent the level of National Emergency, whereby the incident poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of (…) persons. In numerical categorizations, category 4 on a scale of 1-6 may represent a Substantial

Incident and be defined as a cyber attack which has a serious impact on a medium-sized organization, or which poses a considerable risk to a large organization or wider / local government.

REVIEW PROCEDURES

RECOMMENDATION 9

Once established, a cyber incident classification system should be regularly reviewed to assess its effectiveness and ensure it is appropriately informing a country's incident response and its risk or emergency management posture.

Any changes to the incident classification schema deriving from the review process should be introduced in a manner that allows for long-term comparative analysis.

Ideally, once established, a cyber incident classification system should be regularly reviewed to assess its scope and effectiveness and ensure it is appropriately informing a country's incident response and its risk or emergency management posture. To date, across the OSCE region only a few review their NCICS with some frequency. Approaches to the review process vary across countries. In some cases, legal or planning requirements stipulate fixed terms for reviewing the system (every semester, annually, bi-annually), while in others the review process is more organic, carried out whenever optimal or in accordance with the outcome of an assessment or validation of the system.

A requirement to carry out a regular review of the process and system can be included in national legislation (e.g., national information security act), regulatory or guidance documents and may be tied to broader reviews of national cyber incident response or national emergency plans. Lessons from regular exercises to test the national cyber emergency plan could potentially form the basis of the review process.

In instances where there is no obligation or requirement to periodically review the cyber incident classification system, reviews can take place organically when necessary.

Regardless of the approach, it is important that any changes to the incident classification system deriving from a review process should be introduced in a manner that allows for long-term comparative analysis.

CAPACITY AND RESOURCE REQUIREMENTS

Continuous political commitment, skilled personnel, adequate and stable budgets, and review procedures are required to develop, manage and sustain a NCICS.

RECOMMENDATION 10

Continuous political commitment, skilled personnel, including a dedicated incident response entity or team with sound expertise in both general and cyber crisis management, and adequate and stable budgets are critical to the development and management of cyber incident classification systems.

The prior existence of the relevant policy base, legal authorities and requirements and a dedicated incident response entity or team with sound expertise in both general and cyber crisis management are perceived as important pre-conditions to ensuring the effective management of the system and for securing adequate human capital and resources.

Developing, managing and sustaining a classification system also requires inter-personal skills since agreeing on a classification system that serves the purpose of a broad range of organizations and constituents involves a significant amount of engagement (via meetings, workshops, exercises etc.) of public and private actors across a range of sectors and services both during the development and implementation of the system. This can serve an important trust-building function.

Managing and Sustaining Cyber Incident Classification Systems

Inter-agency co-operation

Skilled personnel

Legal authorities

Adequate and stable budgets

Policy framework

Crisis management skills

Political commitment

Inter-personal skills

Review procedures

Public-private collaboration

Communication skills

RECOMMENDATION 11

Engagement of relevant stakeholders and constituencies in the development of the classification system can contribute to building trust between public and private actors and within and across sectors and services.

The development of a classification system can be time and resource intensive in its initial phases and rollout, requiring significant technical expertise for the development of the classification system (e.g., defining the qualitative categories for the incident assessment, priority assignment etc.), as well as significant engagement of other entities and stakeholders in the process. Different tools, procedures, documents will then need to be put in place and information about the new (or reviewed) classification system communicated to its constituents and the broader public. Once agreed and these steps become embedded in national emergency or incident management frameworks or plans, the resources required to sustain it are minimal.

Importantly, the capacities and resources required to sustain a cyber incident classification system are also influenced by its design, including whether its technical component is developed in-house or is out-sourced (e.g., if it is a subscription-based model) and whether it needs to be regularly upgraded in line with changes in cyber incident types. In this regard, cost and efficiency will be a constant factor.

The types of expertise required to develop, manage and sustain the system can include: political, technical, subject-matter, country-specific, legal and communications expertise.

Core duties that are required to manage and sustain the system once developed and that would need to be budgeted for can include:

- Communication and promotion of the system across organizations and constituencies.
- Periodic review of the classification system (categories, scoring etc.) and its effectiveness.

- Regularly exercising the system to build resilience to incidents and test its effectiveness and the preparedness of relevant stakeholders.
- Regular generation of statistics and reports.
- Regular analysis of statistics to understand anomalies in the system (e.g., if too many incidents are registered under ‘Other’, said incident may require a new classification).
- Continuous interpretation and communication of results to the target audience in a timely, consistent and clear manner.
- Comparative analysis of classification standards and systems across countries and regions.

CHALLENGES IN DEVELOPING AND IMPLEMENTING NATIONAL CYBER INCIDENT CLASSIFICATION SYSTEMS

It would be presumptuous to assume that cyber incident classification systems come without challenges. The challenges that OSCE participating States have identified vary significantly, reflecting in part the level of maturity of each country’s classification system. Challenges include:

- Developing a taxonomy that is meaningful and can be used across different entities and sectors;
- Maintaining objectivity in the design of the system;
- Sustaining the iterative process of categorizing and prioritizing incidents;
- An absence of regulation or relevant requirements to ensure that incidents are reported or notified to the relevant body;
- Setting reporting/notification thresholds and implementing related requirements;
- A limited number of qualified and experienced personnel to maintain the system; and
- A lack of awareness of the system or understanding of how it works.

Another identified challenge relates to the categorization and prioritization of incidents. Even the best classification system cannot include all the different possible incident categories. Sometimes, however, an incident does not fit into a certain category or can fit into multiple categories, creating obstacles for triaging an incident. Protocols for determining how to proceed in such situations may therefore be required.

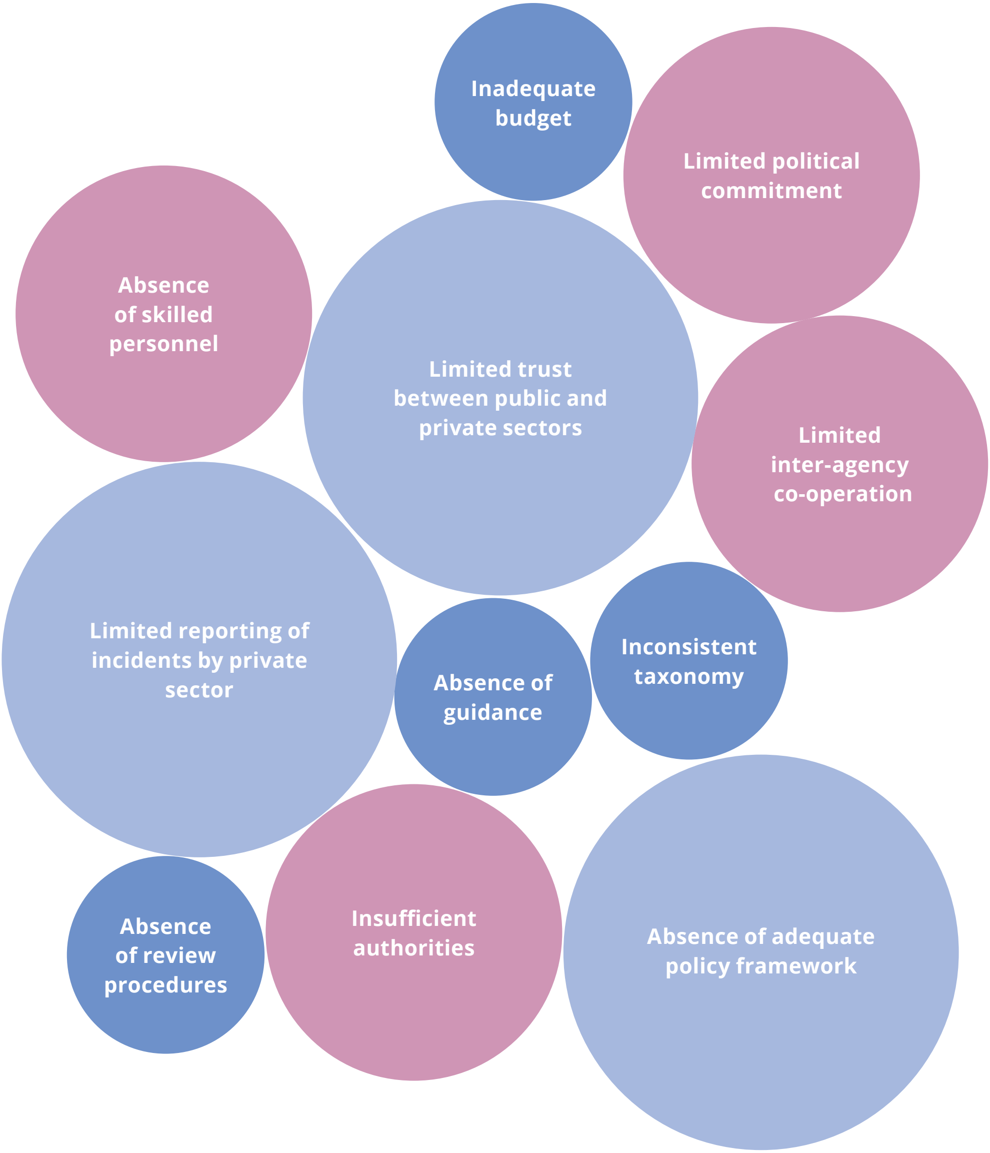
RECOMMENDATION 12

It is important to establish protocols that determine how to proceed when challenges relevant to categorization of incidents are encountered.

The challenge of setting meaningful thresholds for classifying incidents in a manner that can then be interpreted by relevant stakeholders requires specific attention. Since there are many ways of looking at an incident and different actors generally have different information at their disposal, it is often challenging to achieve a common picture of the incident. A lack of specific information provided by target organizations relevant to an incident often requires further interaction to fully leverage the classification scheme. Furthermore, the dynamic, non-static aspect of cyber incidents is not necessarily catered for in current approaches. In this regard, decisions regarding the category and priority assignation of a given incident is generally based on the information that the incident handler has at a given moment. However, said information can change as time passes, which may in turn change the priority level of the incident.

Terminology continues to pose challenges, since many terms in and of themselves do not have a delimited meaning. An example of how to overcome this challenge includes developing a list of definitions and concepts that is then included in the relevant legal instrument or guidance document, although this might become a challenge too, if too narrow in scope.

Challenges



Inadequate budget

Limited political commitment

Absence of skilled personnel

Limited trust between public and private sectors

Limited inter-agency co-operation

Limited reporting of incidents by private sector

Absence of guidance

Inconsistent taxonomy

Absence of review procedures

Insufficient authorities

Absence of adequate policy framework

Ensuring that relevant stakeholders and constituencies not only understand the categories and thresholds of a given classification system, but also report incidents when they are affected is a continuous challenge. Sometimes this may be due to reputational concerns. It may also be because the affected entity does not have an effective risk management model in place and may not have the capacity or resources to carry out proper assessments of the impact of the incident (on the service affected, the number of users affected, the area affected and the impact of the incident on other services or sectors).

Finally, the absence of relevant guidance on category definitions, roles and responsibilities or what a response within a given category entails, constitutes a specific challenge to understanding how the system should be used.

States are overcoming many of the challenges discussed above through the adoption of targeted regulation (for instance, by requiring critical infrastructure operators and owners to report cyber incidents and ransomware payments),; through the provision of more detailed guidance to stakeholders and constituents, and by regularly testing and reviewing their classification system, including through regular exercises and training. Some States are also introducing regulatory requirements where incident notification and reporting is concerned.

2.3 International Co-operation

This section of the report explores potential co-operative measures around national cyber incident classification systems, including openness to sharing the national approach—or elements thereof—to incident classification. It presents views on the existence and value of capacity building in this area, as well as the views on voluntarily participating in dedicated exchanges, including crisis management exercises relevant to cyber incident classification.

EXCHANGES ON NATIONAL APPROACHES TO CYBER INCIDENT CLASSIFICATION

Beyond establishing common and transparent processes and procedures for classifying cyber incidents at the national level, it is broadly accepted that voluntarily sharing national approaches to classifying ICT incidents in terms of the scale and seriousness of the incident with other States can contribute to building confidence between States and help avoid potential misunderstandings that may emerge around cyber incidents and related response measures.

RECOMMENDATION 13

Sharing national approaches to classifying ICT incidents in terms of the scale and seriousness of the incident with other States can contribute to building confidence between States and help avoid potential misunderstandings that may emerge around cyber incidents and related response measures, thus contributing to regional and international security and stability.

Exchanging experiences and sharing information with other states can also be a valuable contribution to the development, testing and maturing of cyber incident classification systems. It can enhance incident management and response, ensure a more common understanding of existing and evolving threats, while also contributing to the broader goal of trust and confidence building.

Exchanges could also take the form of workshops or meetings where lessons and good practices in cyber incident classification and on the different taxonomies are shared. This could help expand existing taxonomies to cover those used by other countries as well as those developed by private actors or research institutes.

There are, however, challenges to participating in dedicated exchanges and exercises. These include capacity constraints and staffing requirements, especially those experienced by smaller countries or those with limited resources. Nonetheless, most States agree that a possible starting point could be information exchanges on national approaches to incident classification.

A range of formats can be used to share national approaches to cyber incident classification. These include making relevant information (policies, regulation, etc.) publicly available on government websites; using existing multilateral platforms or processes, bi-lateral or multistakeholder dialogues; or in-person or online workshops.

CAPACITY BUILDING AND OTHER INITIATIVES RELEVANT TO NATIONAL CYBER INCIDENT CLASSIFICATION

Cyber-security-related capacity building needs remain poorly addressed across the globe, including where cyber incident classification is concerned. In the OSCE region many States view this as a gap that needs to be filled. Crisis management scenarios and table top exercises can play an important role in this regard, and could potentially be tied to a Points of Contact Network, where appropriate.

Chapter 3

Recommendations

Purpose and objectives

The purpose of a NCICS is to generate a clear picture of the cyber threat landscape, ensure a prompt response to cyber/ICT incidents, and minimise the damage they cause. A NCICS supports national crisis management by providing a routine and consistent mechanism to objectively assess the risk of a cyber incident in the national context, in a timely manner and detect possible gaps in defences.

Policy and legal base

Cyber incident classification systems are generally anchored in national policy and other relevant frameworks and often flow from national legislation.

A sound policy and/or legal base for cyber incident classification is critical to ensuring its effectiveness as well as its sustainability.

Establishing clear criteria to determine the stakeholders or constituencies that a national cyber incident classification will serve, including how critical they are to society and economy requires serious consideration. The approach should be flexible enough to accommodate new stakeholders and constituents as the threat landscape changes.

Uniform and consistent reporting on incidents is critical to the effectiveness of cyber incident classification systems and helps determine the nature of the response. In some jurisdictions and depending on the severity of an incident and the entity affected, incident reporting is legally required.

Clearly articulated guidance contributes to the effective implementation and socialization of a cyber incident classification system. Such guidance can specify:

- The purpose of the cyber incident classification system and its policy and/or legal basis;
- Who co-ordinates its development and implementation;
- Its scope/coverage in terms of its key stakeholders/constituencies;
- Definitions and explanations of categories and priorities;
- The response mechanisms for incidents, including an explanation of what would activate a specific classification, which organization responds and what actions they would take; and
- How regularly the incident classification system is reviewed and what the review process entails.

Process and institutional arrangements

Cyber incident classification is generally a centralised process co-ordinated by a central entity or authority and can involve a range of government bodies. Depending on the context, it may also include essential services/critical infrastructure asset owners or operators, digital service providers and other relevant private sector entities.

Engaging relevant stakeholders and constituencies in the design and development of the classification system can contribute to building trust between public and private actors and within and across sectors and services from the outset.

A standard approach to categorizing and prioritizing cyber incidents in accordance with their severity and scale is important for diagnosing an incident and relating the importance of the incident to its impact on a specific institution, entity or sector and its urgency, relative to the timing of the incident. Categorization speeds up the process of incident classification and creates greater efficiency within the process flow while priority assignment can help ensure a common lexicon when an incident is being discussed, help determine urgency, incident response and reporting and notification requirements, as well as recommendations for leadership engagement.

Ensuring clarity on the scope or coverage of a cyber incident classification system, including by establishing clear criteria to determine its key stakeholders and constituents is important, particularly for notification and reporting purposes. The system should remain flexible enough to accommodate an ever-changing threat landscape and include pprotocols that determine how to proceed when challenges relevant to categorization of incidents are encountered. Uniform and consistent procedures for incident notification and reporting is critical to the effectiveness of cyber incident classification systems.

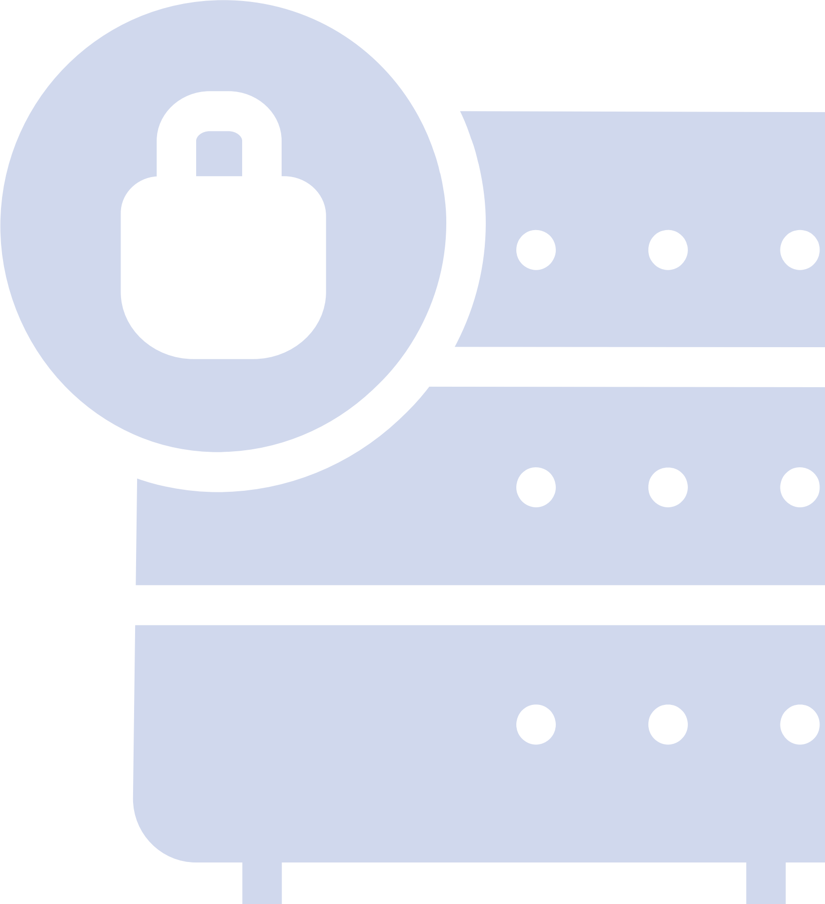
Regular reviews of a NCICS are necessary to assess its scope and effectiveness and ensure it is appropriately informing a country's incident response and its risk or emergency management posture. Any changes to the incident classification system deriving from the review process should be introduced in a manner that allows for long-term comparative analysis.

Sharing national approaches to classifying ICT incidents in terms of the scale and seriousness of the incident with other States can contribute to building confidence between States and help avoid potential misunderstandings that may emerge around cyber incidents and related response measures, thus contributing to regional and international security and stability.

People and resources

Continuous political commitment, skilled personnel, including a dedicated incident response entity or team with sound expertise in both general and cyber crisis management, and adequate and stable budgets are critical to developing, managing and sustaining cyber incident classification systems.

This short study demonstrates that OSCE participating States are affording greater attention to cyber incident classification within their broader incident and crisis management efforts. The report provides valuable insights into existing and emerging practices in the OSCE region in this regard. The aim of documenting these insights and practices is to use the knowledge derived from experiences of participating States to promote the use of incident classification systems nationally and regionally as a means to advance crisis management procedures and address challenges to national and transborder ICT networks, in the spirit of CBMs 15 and 3.



Chapter 4

Concluding Remarks

Experiences in designing these systems vary significantly across OSCE participating States, yet the study clearly demonstrates that common baselines are critical to effective cyber incident management at the national level, and for engaging on cyber incidents regionally and internationally. Some participating States have had incident classification systems in place for quite some time and have developed sound legal and/or policy bases to ensure their effective co-ordination and management as well as adequate resource allocation. For some participating States also members of other organizations such as the EU, existing regulation (e.g., the NIS Directive) has accelerated the establishment of incident classification systems, many of which are now coming into their own. Other participating States are undertaking the first steps toward establishing an incident classification system, while yet others are planning to establish one within the next two years.

It is clear from the experiences discussed that a common classification taxonomy is key to ensuring the effectiveness of any cyber incident classification system. It needs to be clearly communicated to all intended constituencies on a regular and timely basis. Furthermore, establishing and nurturing interagency co-operation and information sharing adds to the effectiveness. Equally important is ensuring regular reviews of the system and allowing enough flexibility to adapt it to shifting circumstances.

Regardless of the stage of development and implementation of their NCICS, the study presents some important emerging practices and lessons across the four categories of purpose, policy, processes and people.

Further exchanges on these will be of immense value not only to OSCE participating States as they continue their efforts to operationalize CBMs 3 and 15, but also to countries in other regions who are in the process of operationalizing recommendations of the UN Open-Ended Working Group and Groups of Governmental Experts on the international ICT security.

Finally, it is important to recall that the cybersecurity threat landscape is continuously shifting and that cyber incident classification systems continue to mature. Notwithstanding, there is sufficient experience, both in the region and globally, in developing and implementing these systems today to allow for valuable exchanges on lessons and practices, including through workshops or capacity building and crisis management exercises.

Annexes
Annex 1 – OSCE Permanent Council Decision No. 1202

Organization for Security and Co-operation in Europe PC.DEC/1202
Permanent Council 10 March 2016

Original: ENGLISH

1092nd Plenary Meeting
PC Journal No. 1092, Agenda item 1

DECISION No. 1202
OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as "security of and in the use of ICTs." They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

The following CBMs were first adopted through Permanent Council Decision No. 1106 on 3 December 2013:

1. Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.

2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.

3. Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.

4. Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.

5. The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.

6. Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

7. Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.

10. Participating States will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

11. Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals from the Consolidated List circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

The following CBMs were first adopted through Permanent Council Decision No. 1202 on 10 March 2016:

12. Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level;

this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.

With respect to such activities participating States are encouraged, *inter alia,* to:

– Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;

– Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and

– Take into account the needs and requirements of participating States taking part in such activities.

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.

13. Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.

14. Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.

15. Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.

Collaboration may, *inter alia,* include:

- Sharing information on ICT threats;
- Exchanging best practices;
- Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;
- Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;
- Sharing national views of categories of ICT-enabled infrastructure States consider critical;
- Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and
- Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.

16. Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments ofthe ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication.

Practical Considerations[1]

The provisions of these Practical Considerations do not affect the voluntary basis for the activities related to the aforementioned CBMs.

Participating States intend to conduct the first exchange by October 31, 2014, and thereafter the exchange of information described in the aforementioned CBMs shall occur annually. In order to create synergies, the date of the annual exchanges may be synchronized with related initiatives participating States are pursuing in the UN and other fora.

The information exchanged by participating States should be compiled by each of them into one consolidated input before submission. Submissions should be prepared in a manner that maximizes transparency and utility.

Information may be submitted by the participating States in any of the official OSCE languages, accompanied by a translation in English, or only in the English language.

Information will be circulated to participating States using the OSCE Documents Distribution system.

Information will be circulated to participating States using the OSCE Documents Distribution system.

Should a participating State wish to inquire about individual submissions, they are invited to do so during meetings of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 or by direct dialogue with the submitting State making use of established contact mechanisms, including the email contact list and the POLIS discussion forum.

The participating States will pursue the activities in points 9 and 10 above through existing OSCE bodies and mechanisms.

The Transnational Threats Department will, upon request and within available resources, assist participating States in implementing the CBMs set out above.

[1] First adopted as part of Permanent Council Decision No. 1106 on 3 December 2013.

In implementing the CBMs, participating States may wish to avail themselves of discussions and expertise in other relevant international organizations working on issues related to ICTs.

Considerations[2]

Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039, to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals for CBMs aimed at increasing transparency, co-operation, and stability among States in the use of ICTs. Such efforts should, to the extent that they relate to the mandate of the IWG, take into account and seek to complement the expert-level consensus reports of the 2013 and 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including their recommendations on voluntary CBMs, and the Group's work in support of voluntarynon-binding norms, rules and principles of responsible State behaviour in the use of ICTs.

The Transnational Threats Department of the OSCE Secretariat, through its Cyber Security Officer will, upon request and within available resources, assist participating States in implementing the CBMs set out above, and in developing potential future CBMs.

[2] First adopted as part of Permanent Council Decision No. 1202 on 10 March 2016.

Annex 2 – Publicly available documents shared by OSCE participating States on national cyber incident classification systems

OSCE participating States	Publicly available document (title/link)
Albania	https://cesk.gov.al/publicAnglisht_html/wp-content/uploads/2016/04/Kategorite%20e%20incidentit.pdf
Austria	https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2018_1_111/ERV_2018_1_111.html https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2019_2_215/ERV_2019_2_215.html
Canada	https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html
Croatia	https://www.cert.hr/wp-content/uploads/2018/06/National-taxonomy-for-computer-security-incidents.pdf https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf https://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/Act%20on%20cybersecurity%20of%20operators%20of%20essential%20services.pdf https://www.uvns.hr/en/legislation/information-security-290/cyber-security
Czech Republic	https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
Estonia	https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf
France	http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf
Iceland	https://cert.is/leidbeiningar/tilkynningar-um-atvik-og-ahaettu/mat-a-alvarleika-atvika/ https://www.almannavarnir.is/english/general-information/emergency-response https://cert.is/leidbeiningar/tilkynningar-um-atvik-og-ahaettu/flokkunarfraedi-atvika/

Latvia	https://likumi.lv/ta/en/en/id/304284 https://likumi.lv/ta/en/en/id/220962
Luxemburg	https://www.govcert.lu/en/ncert/ https://www.circl.lu/pub/taxonomy/
Poland	http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180002180 https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf https://cert.pl/raporty-roczne/ https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/974 https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/974,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2020-roku.html https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180002180 https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32018R0151
Portugal	https://www.cncs.gov.pt/pt/certpt/taxonomia/ https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf

Follow OSCE

OSCE Secretariat
Transnational Threats Department
Wallnerstrasse 6
1010 Vienna, Austria

OSCE Organization for Security and Co-operation in Europe

cybersec@osce.org
www.osce.org/secretariat/cyber-ict-security