Report on the description of RCDC CTI service model

REGIONAL CYBER DEFENCE CENTRE

NRD Cyber Security

Report on the description of RCDC CTI service model

Contents

1 / Preface

The Regional Cyber Defence Centre (RCDC), under the National Cyber Security Centre, has contracted NRD Cyber Security to provide professional services for the development of a Report on description of the RCDC Cyber Threat Intelligence (CTI) model.

This report provides a detailed analysis and description of the RCDC's Cyber Threat Intelligence Service (CTIS), including description of the legal background, mission, vision, benefits, key CTI service procedures and workflows.

This report was prepared by Dr Tadas Jakstas, Team Leader, Dr Vilius Benetis and Ms Donata Judickaitė, Team Members of the Project Team.

2 / List of Acronyms

Term/abbreviation	Meaning/explanation
CNI	Critical National Infrastructure
CTAC	Cyber Threat Analysis Cell
CTI	Cyber Threat Intelligence
CTIS	Cyber Threat Intelligence Service
IR	Intelligence Requirements
Policy	A set of high-level governing principles to a specific subject
Procedure	A written outline of the course of actions to be taken to perform a given task
Process	An organized set of activities which uses resources to transform inputs to outputs
Project	Consultancy Services for the development of the report on description of the RCDC CTI service model
MISP	Malware Information Sharing Platform
MoD	Ministry of Defence
MoU	Memorandum of Understanding
NRD CS	UAB NRD CS (NRD Cyber Security)
OSINT	Open-Source Intelligence
PIR	Priority Intelligence Requirements
RCDC	Regional Cyber Defence Centre
RFS	Request for Support
SIR	Specific Intelligence Requirements
SOP	Standard Operating Procedure
TIP	Threat Intelligence Platform
TTP	Tactic, Techniques and Procedures

3 / Introduction

3.1 Context and General Objectives of the Project

The Regional Cyber Defence Centre (RCDC) established as a joint initiative of Lithuania and the United States aims to fill the niche of multilateral practical cooperation in the field of cyber defence and to strengthen the capacity of both Lithuania and regional partners to ensure cyber security of critical infrastructure of the state. The RCDC develops its activities in three main directions: cyber threat analysis, organisation of exercises for critical infrastructure managers, and practical research. One of the main tasks of the RCDC is to create and effectively develop CTI service in order to enhance operational capabilities of its partners to analyse and withstand cyber threats effectively.

The overall objective of the Project is to **contribute to the implementation of RCDC activities by developing a report on the description of the RCDC's Cyber Threat Intelligence Service (CTIS).**

This intervention aims to **strengthen RCDC CTI activities** by providing a coherent, holistic, strategic and actionable approach for the development of a CTI service. It is expected that this intervention will result in several key outcomes for the RCDC:

1. **Enhanced understanding** of the RCDC mandate and responsibilities in the field of CTI.
2. **Identified and defined key processes** for the RCDC CTI service.
3. **Raised awareness** for partners and the wider public on the main principles and values of the RCDC's CTI Service model.

3.2 Aim of the Report

This Report provides a detailed analysis and description of the legal background, mission, vision, and benefits of the RCDC CTI activities. In addition, the document lists and describes the main RCDC stakeholders. Next, the Report defines the RCDC's Cyber Threat Intelligence Service (CTIS) through service model (FIRST.org's CSIRT Services Framework), including the description of key CTI service procedures and workflows.

3.3 Legal Background

Establishment of RCDC CTI activities is supported by the following bilateral and multilateral documents/agreements:

4. The Memorandum of Understanding (MoU) between the Ministry of National Defence of the Republic of Lithuania, the Ministry of Defence of Georgia and the Ministry of Defence of Ukraine, signed in July 2021, which established the RCDC's Cyber Threat Analysis Cell (CTAC) and set forth the preconditions for its operation, funding, manning, equipping and infrastructure.
5. The Defense Cooperation Strategic Roadmap for 2020 – 2024 between the Ministry of National Defence of the Republic of Lithuania and the Department of Defense of the United States of America, signed on 2 April 2019, which underlines the focus on joint efforts in building capabilities together to deter and defend against malicious cyber intrusions and attacks as well as on close cooperation in improving intelligence sharing[1].
6. The Bilateral Cooperation Roadmap in Cybersecurity Field for 2020 – 2024 agreed upon between the Ministry of National Defence of the Republic of Lithuania and the United States European Command (USEUCOM) which addresses the objective to jointly develop the Regional Cyber Defence Centre (RCDC) as a main cooperation platform and a competence hub.

[1] https://www.defense.gov/News/News-Stories/Article/Article/1803578/us-lithuania-detail-roadmap-for-cooperation- through-2024/

7. The Declaration of Intent[2] on Cyber Security Cooperation between the Ministry of National Defence of the Republic of Lithuania and Ministry of Defence of Georgia signed on 8 March 2019 and the Declaration of Intent[3] between the Ministry of National Defence of the Republic of Lithuania and the Ministry of Defence of Ukraine on Cyber Security Cooperation signed on 27 November 2021, that express the intention to seek a mutually beneficial co-operation in cybersecurity, exchange information and data on cyber incidents and attacks, and pursue mutually beneficial cooperation at the Regional Cyber Security Centre.
8. The existing agreements between the RCDC-participating countries regarding Mutual Protection of classified information and applicable NATO rules governing the protection of classified information.

4 / Mission[4] and Vision

When it comes to CTI part, the **RCDC's vision** is:

> **"Significantly increase cyber security capabilities of the participant states, effectively use international cyber threat analysis capabilities".**

According to the Memorandum of Understanding (MoU) between the Ministry of National Defence of the Republic of Lithuania, the Ministry of Defence of Georgia and the Ministry of Defence of Ukraine, signed in July 2021, the **RCDC's CTAC mission** is:

> **"To develop multinational cyber threat analysis capacities by developing standard practices for information sharing on cyber threats, security vulnerabilities, incident handling, and digital forensics at operational and tactical level".**

5 / RCDC CTAC Advantages

A successful implementation of RCDC CTAC activities will bring the following **benefits**:

1. Knowledge and experience-sharing.
2. Information merging and sharing.
3. Focus on sectors of interest defined by participating organizations.
4. Strengthened preventative defence operations for each entity.
5. Strengthened bonds between nations through international collaboration.

[2] https://www.lrp.lt/en/media-center/news/lithuania-and-georgia-join-efforts-to-respond-cyber-attacks/31975

[3] http://kam.lt/en/news_1098/current_issues/lithuania_and_ukraine_intensifies_cooperation_on_cybersecurity.html

[4] Please note that the scope of this report is limited to defining the mission and vision specifically of the RCDC's CTI activities.

6 / Introduction of partners

The RCDC stakeholder organizations are listed in the table below with the interest in the RCDC CTAC performance and the role in the relationship with the RCDC's CTAC identified clearly:

Table 1 List of stakeholders

#	Stakeholder	Type of stakeholder	Role in the relationship with the RCDC CTAC	Interest in the RCDC CTAC
1.	The National Cyber Security Centre of Lithuania (NCSC) under the Ministry of National Defence of Lithuania	RCDC-hosting organisation	Provision of organisational structures, budget, and other resources for RCDC operations. Sharing information on national and cross-border cyber security threats required in support of the CTAC objectives in a proactive and timely manner.	To use the analytical CTI products developed by the RCDC to enhance the resilience of CNI. Enhance the image of Lithuania as one of the leading countries in the area of cybersecurity.
2.	Ukrainian MoD	MoU-based partner	Sharing information on national and cross-border cyber security threats required in support of the CTAC objectives in a proactive and timely manner.	To use the analytical CTI products developed by the RCDC to enhance the resilience of CNI.
2.1.	Signal Corps and Cyber Security Command of the Armed Forces of Ukraine	MoU-based partner	Sharing information on national and cross-border cyber security threats required in support of the CTAC objectives in a proactive and timely manner.	To use the analytical CTI products developed by the RCDC to enhance the resilience of CNI.
2.2.	Defence Intelligence of Ukraine	MoU-based partner	Sharing information on national and cross-border cyber security threats required in support of the CTAC objectives in a proactive and timely manner.	To use the analytical CTI products developed by the RCDC to enhance the resilience of CNI.
3.	Georgia MoD	MoU-based partner	Sharing information on national and cross-border cyber security threats required in support of the CTAC objectives in a proactive and timely manner.	To use the analytical CTI products developed by the RCDC to enhance the resilience of CNI.
3.1.	Cyber Security Bureau under Georgia MoD	MoU-based partner	Sharing information on national and cross-border cyber security threats required in support of the CTAC objectives in a proactive and timely manner.	To use the analytical CTI products developed by the RCDC to enhance the resilience of CNI.

#	Stakeholder	Type of stakeholder	Role in the relationship with the RCDC CTAC	Interest in the RCDC CTAC
4.	Pennsylvania National Guard of the United States of America	Full-fledged partner	Sharing information on national and cross-border cyber security threats required in support of the CTAC objectives in a proactive and timely manner.	To use the analytical CTI products developed by the RCDC to enhance the resilience of CNI.
5.	Cybersecurity and Infrastructure Security Agency	Trusted partner	Sharing public information on national and cross-border cyber security issues[5], including threats and vulnerabilities. Cooperate with the RCDC in organising CTI public events, research, training and education activities.	To use publicly accessible RCDC CTI analytical products.

7 / RCDC Cyber Threat Intelligence Service (CTIS)

Presented below is the description of the CTIS which is further broken down into process, procedures and workflow models.

The RCDC's mandate (authority and responsibility) is implemented via CTIS, offered to stakeholders/partners.

Table 2 Description of CTIS

No.	Name of the Service	Description
1.	RCDC Cyber Threat Intelligence Service (CTIS)	The RCDC Cyber Threat Intelligence Service (CTIS) covers threat intelligence processing, analysis, and production. Additionally, a cyberthreat intelligence platform is provided for community sharing and information exchange.

7.1 CTIS Process, Procedures and Workflows

The CTIS is defined by the process below.

The CTIS process consists of four procedures represented by workflow diagrams, depicting each step from the start until the final phase of activity.

[5] Please note that the scope of this report is limited to defining the mission and vision specifically of the RCDC's CTI activities.

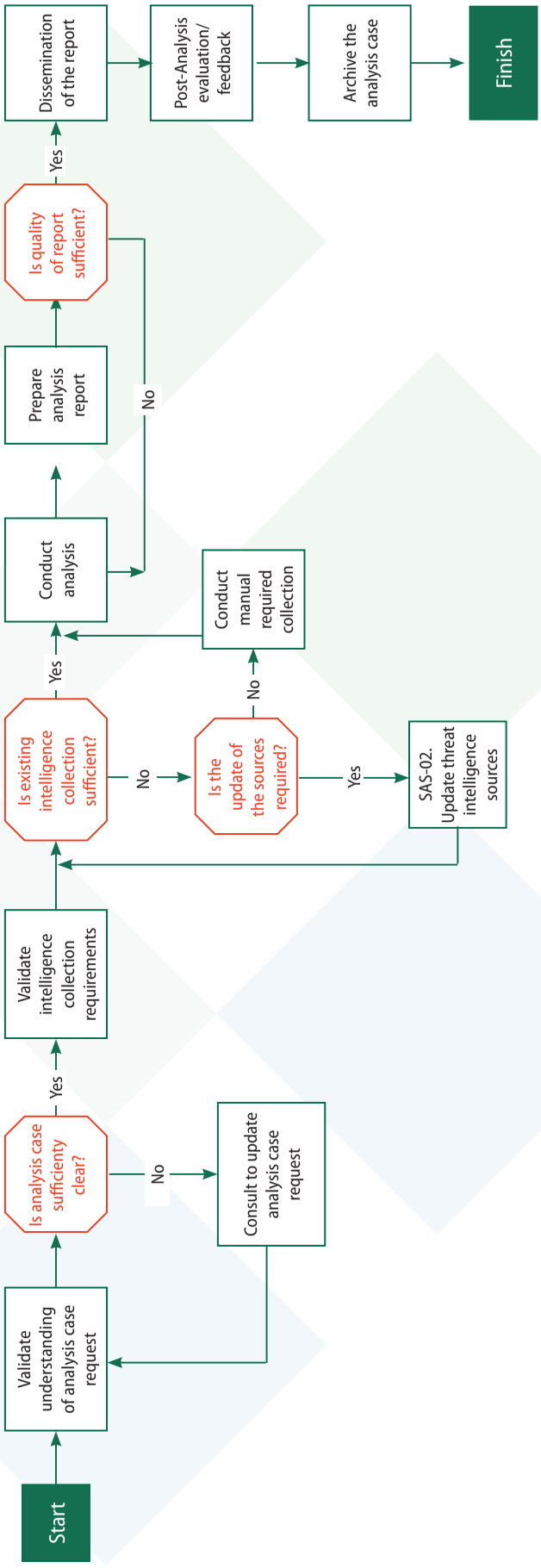
Table 3 CTIS Process Description

Process Attribute	Description
Name	RCDC CTIS Process
ADMINISTRATOR	Head of CTAC
Purpose	To ensure that the RCDC is able to process, analyse, produce, and share actionable and timely CTI products with partners.
Input/triggers	1. Approved RCDC Annual Activity Plan. 2. Individual CTI analysis request by the head of CTAC. 3. Identified CTI information collection deficiency(ies)/gap(s). 4. New threat information received by CTI analysts.
Outputs/deliverables	1. Collection of up to date and relevant intelligence sources. 2. Conduct of a professional CTI analytical process. 3. Dissemination of timely and actionable CTI analytical products (reports, articles, alerts).

The following procedures are considered to define expert work at CTIS service:

1. SAS-01: Threat analysis case management: the main method of work for all analysts, defining work on a case by case basis, and showing the progress from the opening to closing an individual analysis case.
2. SAS-02: Updating threat intelligence sources: a procedure to apply corrections to the active set of intelligence sources – changing, or adding a new one.
3. SAS-03: Threat intelligence information exchange: sharing or becoming familiar with the shared information.
4. SAS-04: Alerting on threat intelligence: the CTIS is to issue critical alerts to the relevant stakeholders via direct channel.

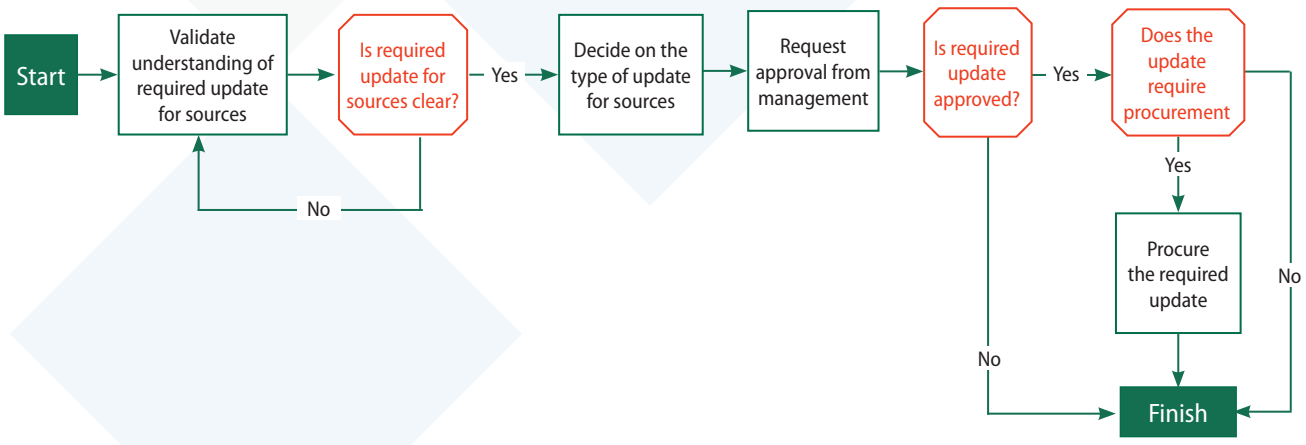
7.1.1 SAS-01: Threat analysis case management



#	Step	Position	Description
1.	**Start**	Agent	The request for an analysis case could be presented with the Department's Annual Activity Plan or it could be initiated by request of the head of CTAC. Associated RCDC CTAC-SOP: **4.8 Reports**
2.	**Validate the understanding of an analysis case request**	CTI analyst	Once the request for an analysis case is received, the CTI analyst responsible for the case management validates the comprehension of the analysis case request.
3.	**Is analysis case sufficiently clear?**	CTI analyst	CTI analyst reviews the analysis case request and decides. **[Yes]** Go to step **"Validate intelligence collection requirements"**. **[No]** Go to step **"Consult to update analysis case request"**. In **[No]** case, the CTI analyst should reach out to the requester of the original analysis case request and clarify the comprehension of the case.
4.	**Validate intelligence collection requirements**	CTI analyst	In case the analysis case is understood sufficiently well, the intelligence collection requirements should be assessed and validated. Once validation of the requirements is done, the analyst should be able to determine: 1. What information/data should be the focus for the collection? 2. What are the main sources of information to collect the information? 3. What are the main tools/techniques to effectively collect the information? Please refer to **Annex 1** for guidelines/recommendations on intelligence requirement and data source alignment.
5.	**Is existing intelligence collection sufficient?**	CTI analyst	CTI analyst reviews the collection requirements for the analysis case and decides whether the intelligence collection is sufficient. **[Yes]** Go to step **"Conduct analysis"**. **[No]** Go to step **"Is an update of sources required?"**.
6.	**Is the update of intelligence sources required?**	CTI analyst	In case the existing intelligence collection is not sufficient, the CTI analyst decides whether **an update of intelligence sources is required**. **[Yes]** Go to step **"SAS-02 Update threat intelligence sources"**. For more detail, please refer to SAS-02 procedure. **[No]** Go to step **"Conduct required manual collection"**. Please note that there are various mechanisms for collecting data manually but the key to gaining most value is to ensure that the collection processes are standardised. Key elements of recording manually collected data are: • Date and time • Forecast timescales of relevance • Nature of data gathered • Specific technical records Manual collection should also include assessment of Open-Source Intelligence (OSINT), Dark Web Content, Limited Distributed Content, etc. Please refer to **Annex 2** for the list of data sources used for manual intelligence collection. Please refer to **Annex 3** for guidance/recommendations for evaluation of information content and source reliability based on NATO or Admiralty Code.

#	Step	Position	Description
7.	**Conduct analysis**	CTI analyst	In case the existing intelligence collection is sufficient, the CTI analyst proceeds to the conduct of analysis. Associated RCDC CTAC-SOP: **4.8 Reports** Please refer to **Annex 4** for guidance/recommendations on application of analytical tradecraft to the analysis process.
8.	**Prepare analysis report**	CTI analyst	After completing the analysis, the next step is to streamline all analysed information and to prepare the analysis report. Associated RCDC CTAC-SOP: **4.8 Reports**
9.	**Is the quality of the report sufficient?**	Head of CTAC	Head of CTAC reviews the draft report and decides if the **quality of the report sufficient for dissemination**. **[Yes]** Go to step **"Dissemination of the Report"**. **[No]** Go to step **"Conduct Analysis?"**. Please note that in case of **[No]**, a clear justification why the quality is not sufficient and clear recommendations on whether the drafted report should be revised to ensure appropriate quality have to be provided to the responsible CTI analyst.
10.	**Dissemination of the report**	CTI analyst	Once the quality of the report is approved, the prepared analysis report is disseminated via agreed communication channels.
11.	**Post-analysis evaluation/ feedback**	Agent	Formal mechanisms should be set in place to receive feedback from customers (partners) after the report is published.
12.	**Archive analysis case**	Agent	Once the analysis report is disseminated and the post-analysis evaluation/ feedback process is completed, the analysis case is archived.
13.	**Finish**	Agent	The analysis case is closed.

7.1.2 SAS-02: Update threat intelligence sources

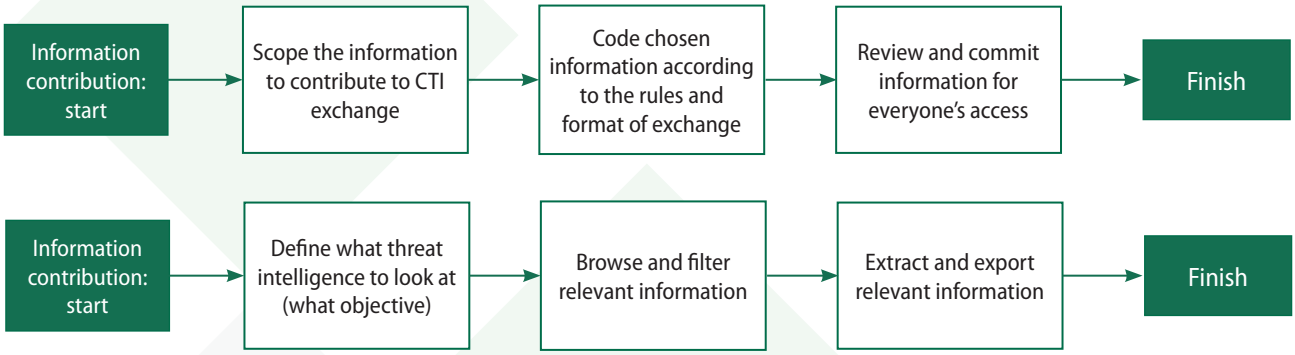


#	Step	Position	Description
1.	**Start**	Agent	A need for an update of intelligence may result from identified information collection deficiencies/gaps during SAS-01: Threat analysis case management or it could be initiated by head of CTAC as a result of required changes of e.g., post analysis/feedback process.
3.	**Validating the assessment of a required sources update**	CTI analyst	Once the information collection deficiencies/gaps are identified, the responsible CTI analyst confirms the assessment of a required sources update.
4.	**Clarification on the required source update**	CTI analyst	CTI analyst reviews the required update for sources and decides whether the update for sources is clear. [**Yes**] Go to step "**Decide on the type of the update required**". [**No**] Go to step "**Confirm the understanding of requested source update**"
5.	**Type of source update**	CTI analyst	In case the requested update for sources is clear, the CTI analyst chooses the type of update required: e.g., general types of updates could be the following: **Modify**: to **change** somewhat the form or qualities of; alter partially; amend. **Add**: to **add** a particular quality **to** something. For example, additional functions **Delete**: to **eliminate** especially by blotting out, cutting out, or erasing.
6.	**Management approval request**	CTI analyst	Once the type of the update required is chosen, a documented request for **the type of an update required** is sent by the responsible CTI analyst to the head of CTAC service. The documented request should provide a clear justification for the required source(s) update, including, among other things, justification of what benefits the update will bring to the analysis process.
7.	**Approval of the required update**	Head of CTAC	Head of CTAC department reviews the update request and approves it or not. [**Yes**] Go to step "**Does the update require acquisition?**" [**No**] Go to step "**Finish**".
8.	**Does the update require procurement?**	Agent	[**Yes**] Go to step "**Procure the required update**". [**No**] Go to step "**Finish**".
9.	**Procure the required update**	Agent	In case the acquisition is required, the procurement process for the required update is completed.
10.	**Finish**	Agent	Threat intelligence sources update is completed.

7.1.3 SAS-03: Threat intelligence information exchange

Threat intelligence information exchange consists of two sub-procedures:

1. Information contribution procedure
2. Information consumption procedure



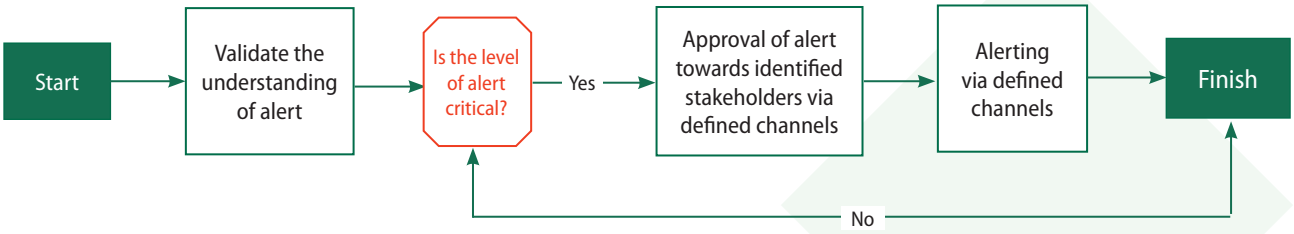
1. Information contribution procedure

#	Step	Position	Description
1.	**Start**	Agent	Information contribution process starts.
2.	**Scope the information to contribute to CTI exchange**	CTI analyst	CTI analyst scopes the information to contribute to CTI exchange.
3.	**Encrypt the chosen information according to the rules and format of exchange**	CTI analyst	The information is coded as required by the rules and format of exchange.
4.	**Review and commit the information for everyone's access**	CTI analyst	CTI analyst reviews and commits information for everyone's access.
5.	**Finish**	Agent	The information contribution process is completed.

2. Information consumption procedure

#	Step	Position	Description
1.	**Start**	Agent	Information consumption process starts.
2.	**Define the threat intelligence to be looked at (the objective)**	CTI analyst	CTI analyst defines what threat intelligence to look for.
3.	**Browse and filter relevant information**	CTI analyst	CTI analyst browses and filters relevant information.
4.	**Extract and export relevant information**	CTI analyst	CTI analyst extracts and exports relevant information.
5.	**Finish**	Agent	The information consumption process is completed.

7.1.4 SAS-04: Alerting on threat intelligence



#	Step	Position	Description
1.	**Start**	Agent	The need for alerting on threat intelligence could come as a result of new threat information received by a CTI analyst.
2.	**Validate the understanding of alert**	CTI analyst	Upon receiving the threat information, the CTI analyst confirms the comprehension of threat alert.
3.	**Is the level of alert critical?**	CTI analyst	The CTI analyst reviews the received information regarding the threat alert and concludes if the level of alert is critical. [**Yes**] Go to step "**Approval of alert towards identified stakeholders via defined channels**". [**No**] Go to step "**Finish**".
4.	**Approval of alert towards identified stakeholders via defined channels**	CTI analyst	In case the level of alert is determined to be critical, the alert is approved for dissemination with relevant stakeholders.
5.	**Alerting via defined channels**	CTI analyst	The alert is being disseminated via defined channels.
6.	**Finish**	CTI analyst	The alerting is closed.

8 / Conclusions

The Regional Cyber Defence Centre, officially established in July 2021, operates as an element of the National Cyber Security Centre under the Ministry of National Defence of Lithuania. In its daily activities, the RCDC focuses on cyber threat analysis, information exchange and practical recommendations.

In this Report, the description of the RCDC CTI service model is provided. The report begins with an overview of the legal foundation, vision, mission, and the main advantages of the RCDC CTAC activities. Further, the main stakeholders of the RCDC's CTI service are introduced by defining their role in the relationship with RCDC, as well as defined interest in the RCDC's CTI performance. Furthermore, the document delineates the RCDC's CTIS model and breaks it down into procedures and workflow models, thus defining the expert work at the CTIS service.

9 / Annexes

9.1 Guidance for Intelligence requirement and data source alignment

It is important for the organization to have a formal repeatable process for aligning data sources to meet intelligence requirements. This process should be reviewed and updated regularly. The list below provides guidelines/best practices for an organization to align data sources to meet intelligence requirements.

Ser. No	Activity	Description
1.	Map data sources to intelligence requirements	Map data sources to their intelligence requirements to align existing and new data sources with existing organizational IRs, PIRs, and SIRs.
2.	Evaluate and communicate with intelligence vendors	Evaluate and communicate intelligence collection requirements by explaining the justification and priority behind them and provide feedback to the third party. For example, some organisations continuously evaluate third-party intelligence providers by scoring criteria, like letter grades. Other organisations track the third-party provider's performance using, e.g., month-to-month graphs to show how intelligence provided by the vendor met the intelligence requirements and helped the organization
3.	Differentiate between third-party intelligence aggregators and intelligence originators	Identify whether the provider is an intelligence aggregator or an intelligence originator. An intelligence aggregator simply collects and passes intelligence to its customers, while an intelligence originator provides new context to the information, making it actionable and relevant to the customer.

Ser. No	Activity	Description
4.	Use a wide variety of sources	Use a variety of internal and external data sources to support intelligence analysis. Internal data sources should include logs, tips, and other information from data sharing-relationships, service level agreements. External sources are both paid and free third-party intelligence providers or platforms that provide aggregated intelligence and/or additional originated context (actionable and organizationally relevant) about atomic, behavioural, and computed indicators of comprise and associated meta-data analysis (email addresses, IP addresses, user agent strings, etc.) related to vulnerabilities, threat actor groups, threat actor TTPs, threat actor capabilities and motivations, and threat campaigns. External intelligence vendors may provide information from a collection of sensitive sources which could include adversary communications in dark/deep/surface web forums, C2 servers, forensic analysis, Virus Total, Shodan, endpoint, and network security data that they have access to from their organizational customers.

9.2 List of data sources for manual intelligence collection

Ser. No	Activity	Description
1.	CTI Sharing Networks	The term CTI sharing networks refers to formal or informal threat intelligence sharing between practitioners. This is a common practice in government departments, for example, networks exist between those who had previously worked in the military or intelligence agencies and are now employed in the private sector, or in government departments. Some of these have developed into more formalised structures. Regardless of origin, sharing intelligence between peers is critical to achieving success, and we encourage all departments to be actively involved in contributing to cross-government threat intelligence. For example, Information Sharing and Analysis Centres (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases, to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.

Ser. No	Activity	Description
2.	Open-Source Intelligence	Open-Source Intelligence (OSINT) refers to the collection of data from publicly available sources such as information on the Internet or in the media. This information is openly accessible for analysts to reach; however, the vast amount of content means that effective curation and management is required. OSINT can include (but is not limited to) content from the following: • Social media: social media can be monitored for threat information being published by researchers, commercial CTI providers or even the spokes-people for threat actor groups themselves. Intelligence gathered from social media must be scrutinised to ensure that the intelligence is accurate, and that is appropriate to collect. • WHOIS: a widely used internet record listing which identifies the owner of a website domain and contact details. The CTI function can use WHOIS data to identify registered users of domain names, blocks of IP addresses or autonomous systems. For any registrant who hasn't opted to mask their information, the registrant's name, address, email and phone number can be searched. For example, threat actors may use registered domains for collecting ransomware payments using their own public email address, thereby unwittingly incriminating themselves, or associating themselves with more than one campaign. • Domains and IP address analysis services: this information can be used to develop information about threat actors that control the infrastructure, including motivation, techniques, objectives, and more. This information can be gleaned from data sources that cross-index large volumes of information about domain registrants and IP address assignees. Various data points, such as domain registrants, IP address owners, DNS data, and more, can surface links between domains. This can help a department to obtain advanced warning of impending attacks where attackers are re-using IT infrastructure. • CVE: Common Vulnerabilities and Exposures (CVE) is a catalogue of known vulnerabilities and the technologies which they relate to. The number of CVEs is growing, and it's relatively simple for a CTI function to enhance its capability by understanding CVEs relevant to its own infrastructure. This information can then be used (along with threat actor profiles identifying which threat actors commonly use which vulnerabilities) to prioritise vulnerability remediation. Anecdotally, it is common for departments to "accept the risk" associated with vulnerabilities which do not have high CVE scores. Enhancing knowledge of threat actor use of CVEs can provide context to that decision, which may affect the outcome of the decision to not remediate the vulnerability. • Shortened URL Processing and Indexing: this is the translation of a long Uniform Resource Locator (URL) into an abbreviated alternative that redirects to the longer URL and understanding subsequent connections. Malicious threat actors use short URLs to conceal the actual URL, and plant malware and phishing links. The short URLs can bypass the security controls which block blacklisted domains, however they can be detected and analysed with appropriate tooling. Once analysed, shortened URLs can be either marked safe, or added to existing threat actor profiles if they redirect to known bad infrastructure.

Ser. No	Activity	Description
3.	Deep/Dark Web Monitoring	The definition of the deep/dark web can be confusing. The deep web is often the part of the internet that average users won't understand accessing (such as the onion router [ToR] or Invisible Internet Project [I2P] sites). This often provides a level of anonymity that can make attribution difficult. There is a lot of content available on the deep web, some of which relates to activities from threat actors. The dark web can be on the surface (regular) internet or on the deep web. However, it has the distinction of being run by threat actors that are actively policing the access and use of these forums and portals to prevent detection/infiltration by agencies, such as law enforcement and intelligence agencies. Whilst there are use cases that require searching for content on the dark web, the clear majority of useful CTI content can be sourced from the open web or from commercial vendors. CTI capabilities should also stay up to date on the ever-changing public list of Tor servers, attackers regularly use Tor as a bridge from their infrastructure to a target, and therefore traffic to and from Tor nodes should be monitored closely.

9.3 Guidance/recommendations for evaluation of information content and source reliability based on NATO or Admiralty code

Trusting data and data sources—identifying what is true and not true and having confidence that data is accurate, is reliable, and hasn't been tampered with—will become a more important challenge in coming years.

A number of high-performing organizations and third-party intelligence providers that generate original context use the NATO or Admiralty Code Grading System for conveying source reliability and credibility of information. The Admiralty Code, which provides a binary rating system that considers the reliability of both sources and the information they provide, is a positive step toward a common lexicon or ontology for data source validation. Additionally, the Admiralty Code is an incorporated taxonomy in the Malware Information Sharing Platform (MISP).

Evaluation of Source Reliability

A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot be Judged	No bias exists for evaluating the reliability of the source

Evaluation of Information Content

A	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject
B	Probably True	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C	Possibly True	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Doubtfully True	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Improbable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot be Judged	No bias exists for evaluating the reliability of the source

9.4 Guidance on the application of analytical tradecraft into analysis process

High-performing organizations incorporate analytical tradecraft into workflows, specifically for performing CTI analysis. It is generally not realistic to apply structured analytical techniques and analytical standards to every threat report. That is simply not feasible or logical when it comes to the speed and demands of mission (such network defence, cyber hygiene and incident response) and other fast-paced (machine and human) generated analysis that leads to immediate and near-term actionable cybersecurity focused recommendations. However, organizations should make informed decisions, pending resources and timing based on threat/event criticality if incorporating analytical tradecraft into Threat Analysis is feasible either before or after mitigation actions are taken. Most reports, at least at the operational and strategic analysis level, should include estimative language, source descriptors or source validation, confidence level, and intelligence gaps.

The table below provides some of alternative analysis techniques used for CTI analytical process:

Ser. No	Alternative analysis techniques	Description	What to use for
1.	**Alternative Futures Analysis**	A technique that systematically explores multiple ways in which a highly complex and uncertain situation can develop. Nevertheless, it does not attempt to predict the future, but to create a thinking context in the form of hypothetical prospects.	• handling situations that are too complex to predict a single outcome for them; • managing high levels of uncertainty.

Ser. No	Alternative analysis techniques	Description	What to use for
2.	**Devil's Advocacy**	A technique that allows an individual or a team to become the critic of a proposed solution, decision, or key assumption. In general, it challenges a single, strongly held view regarding a critically important subject by building the best possible case for an alternative explanation.	• challenging a consensus or key assumption and examining doubts on a widely held view; • making a plan more resilient; • strengthening a decision against close scrutiny; • validating assumptions; • reaffirming your confidence in judgments made on an important issue.
3.	**Team A/Team B Analysis**	A technique that employs separate teams who contrast two or more strongly held views or competing hypotheses. Team A/team B analysis centres on reducing friction and narrowing differences through focused and evidence-based arguments.	• resolving a longstanding strategic issue; • scrutinizing a critical decision with far reaching implications before its implementation; • handling a dispute within a community that has obstructed effective cooperation.
4.	**What-If Analysis**	A technique that assumes an event resulting in a negative or positive outcome has occurred and explores possible explanations how it might have come about. In general, it shifts the focus from whether an event could occur to how it may happen. Contrary to pre-mortem analysis, this method tries to analyse trends and to develop signposts towards future events instead of finding explicit reasons for a potential failure	• identifying the key stakeholders in case of and the issues to address prior to such an event occurring; • understanding how an event may come around in the future; • confronting a confidently made forecast that may not be clearly justified; • questioning a strong mindset that an event may not take place as planned.
5.	**Five Whys**	A technique that aids in identifying the root cause(s) of a problem by asking "why" five times. This is a remarkably simple way to uncover the nature and source of both single-track and multitrack problems. In the former, you face only a single causal chain from your problem to the root cause. In the latter on the other hand, your problem has several initial causes, and you address each one by its own track of "why" questions.	• finding the causes of simple problems and distinguishing them from their symptoms; • determining the relationship between different root causes of a problem.

Issued by the RCDC CTI Service Model Description Report

Layout by the Visual Information Section of the MOD General Affairs Department,
Totorių str. 25, LT-01121 Vilnius. 2022
Printed by the LITHAF Military Cartography Centre,
Muitinės str., Domeikava, LT-54359 Kaunas District.