CYBER4Dev

CIIP TOOLKIT FOR POLICY MAKERS

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Funded by the European Union

Funded by the
European Union

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

Contents

Our Authors

Perit Kirkmann

Perit is a Lead Expert for the Estonian Information System Authority (RIA) specialising in healthcare and the transport sector. Her main responsibilities are critical information infrastructure protection (CIIP) and in particular, developing close working networks with a variety of vital service providers, to help increase the awareness of cybersecurity issues amongst service providers. As part of her work, she also leads several working groups that co-ordinate large parts of the national vital service providers cybersecurity network.

Perit has previously worked as a chief specialist for the Ministry of Social Affairs and the Estonian Health Board where she contributed to Estonian healthcare crisis preparedness and the development of Estonian Emergency Act. Perit supports Cyber4Dev as a short term expert and has conducted training in Critical Information Infrastructure Protection for Rwanda, Costa Rica, Guyana, Cambodia and the Dominican Republic.

Perit has a Bachelor's degree in Law from University of Tartu and a Master's degree in Organisational behaviour from the University of Tallinn.

Priit Kaup

Priit Kaup is a Lead Cyber Security Expert working for the Estonian Information System Authority (RIA). His main responsibilities are critical information infrastructure protection (CIIP) and as such he works closely with a variety of vital service providers to help increase their cyber security awareness and technical capabilities. He also has an extensive background in organising technical security testing and risk management consulting in IT.

Priit supports Cyber4Dev as a short-term expert and has conducted training in penetration testing and Critical Information Infrastructure Protection for countries in Africa, South-East Asia, South-America and the Caribbean.

He has a degree in Information Technology and has studied Cyber Security at both the University of Tartu and at Tallinn University of Technology

Ilmar Toom

Ilmar Toom is Head of the Standards and Supervisory Department in the Estonian Information System Authority, (RIA). The teams he leads have two core functions: the first has responsibility for developing Information Security measures and maintaining standards, the second being responsible for the deployment of supervisory procedures. Ilmar's work in CIIP dates back to the early 2000's when he was engaged in wind energy projects after which he later moved on to industrial wastewater and waste air treatment projects. Latterly, he has held several compliance-related posts both in the public and private sector, where over the past 10 years the emphasis of his work has been on cyber security.

Introduction

What is this toolkit about?

Over the past decade the speed of global digitalisation has provided many of the world's citizens with improved access to services, at a pace that has often left organisations struggling to equip themselves to meet the challenges that it has presented. As services have become ever more digitised, hackers have also developed their capabilities and the impact of cyber attacks upon vital services has increased exponentially during this time.

With states and criminals constantly testing the cyber capabilities of even the most advanced states and organisations, the protection of Critical Information Infrastructure (CII) against cyber attacks has never been more important.

The identification of Critical Information Infrastructure Protection (CIIP) priorities and strategies is a complex but important topic for Governments as members of the public depend on the proper functioning of their Critical Infrastructure (CI) services such as energy supply, telecommunications, financial systems, water and governmental services.

This toolkit helps to give an understanding of the legislative landscape of CIIP, as well as provide ideas on how organisations can develop cyber capabilities that will help them maintain and develop resilience.

What is a vital service?

A vital service is **a service that has an overwhelming impact on the functioning of society and the interruption of which is an immediate threat to the life or health** of people or to the operation of another vital service or service of general interest.[1]

What is critical infrastructure?

The European Union describes Critical Infrastructure CI as an asset, system or part thereof, which is essential for the maintenance of vital societal functions, and the health, safety, security, economic or social well-being of people, and whose disruption or destruction would have a significant impact in a Member State as a result of the failure to maintain those functions (see Council Directive 2008/114/EC»)

Critical infrastructures are the **key systems, services and functions** whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security or any combination of those matters.

These include all major communications, energy, banking, transportation, public health and safety and essential government services.

[1] Emergency Act. Estonia. https://www.riigiteataja.ee/en/eli/ee/513062017001/consolide/current

Governments are increasingly aware of the role critical infrastructures play in supporting the overall economy and security of their nations. It is essential that countries at all stages of development plan for and develop policies that will enable them to provide reasonable assurance of resiliency and security to support key national missions and economic stability.

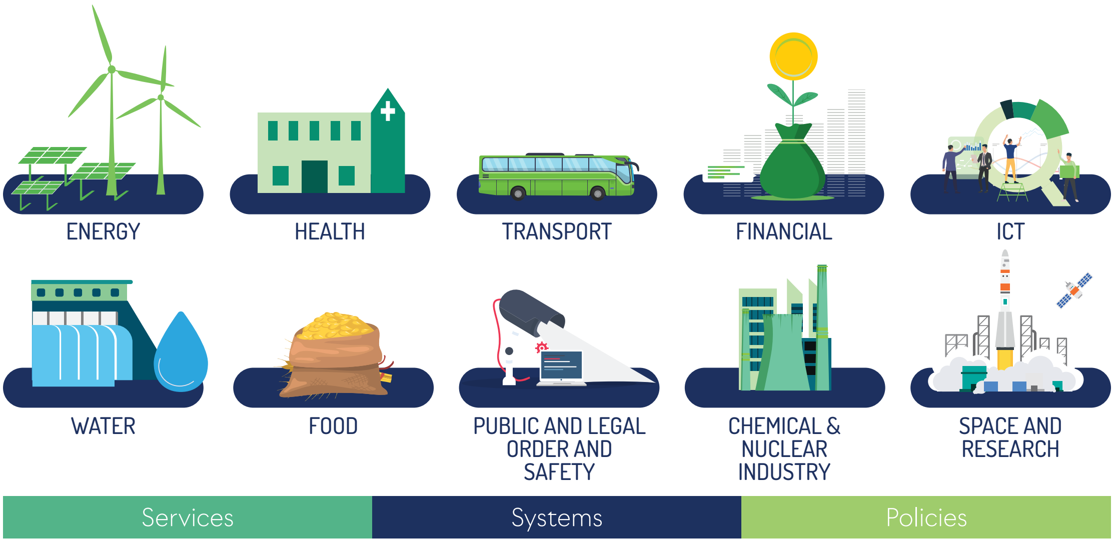
And there are some services that are more important than others. For example, telecommunications and **energy supply** are **the core** resources that cut all lines of national infrastructure. These are the services that other vital services rely on.

What is critical information infrastructure?

Critical information infrastructure (CII) means information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country. The critical information infrastructure is a part of the critical infrastructure.

Critical infrastructures are often thought of as physical assets such as bank buildings, power plants, trains, hospitals and government offices. These physical elements rely upon an often unseen critical information infrastructure and key functions (CII/KF) to actually deliver services and conduct business. Over the past two decades rapid advances in information services and communications technologies have enabled many traditionally separate infrastructures to integrate and automate. The ubiquity and importance of information and communications technology are increasingly recognised as a discernible cross-cutting "critical information infrastructure" upon which all other infrastructures depend. In some sense, the CII/KF are more complex to identify than more established infrastructures such as electric power, because it is composed of systems, processes and services that are not readily identifiable in the way physical elements are. However, because virtually all elements of a nation's economy rely upon it, government and private sector should work together to develop collaborative CIIP frameworks for prevention, detection, response, and recovery.

What underpins all of these functions?



A key takeaway is that **the critical information infrastructure (CCI) is a part of the critical infrastructure (CI) and before we can identify the CII we have to know our CI.**

Why it's important to identify vital services, CIs and CIIs

The services that comprise a country's critical infrastructure are known as the power used in homes, the water we drink, the transportation that moves us, the stores where we shop, and the internet and communications we rely on to maintain our contact with friends, family, and colleagues. Physical and cyber infrastructure is usually operated by the private sector, though some of it can be also owned by state, or local governments. But to keep in mind is that not all infrastructures within an industry sector are critical to a nation or region. It is necessary to identify which infrastructure is both critical to maintain continued services or functions and vulnerable to some type of threat or hazard. Prioritising the allocation of available resources to that subset of infrastructure can enhance a nation's security, increase resiliency, and reduce risk.

There are four designated lifeline functions-transportation, water, energy, and communications, which means that their reliable operations are so critical that a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors. For example, energy stakeholders provide essential power and fuels to stakeholders in the communication, transportation, and water sectors, and, in return, the energy sector relies on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication).

These connections and interdependencies between infrastructure elements and sectors mean that the loss of one or more lifeline function(s) typically has an immediate impact on the operation or mission in multiple sectors. As a result, additional loss of other functions may arise over time. Further, identifying and officially recognizing industry sectors that are lifeline sectors and/or have cross-sector interdependencies facilitates collaboration and information exchange that promotes continuity of operations and services. The choice of sectors prioritized in outreach efforts should reflect an understanding of the infrastructure's interconnectedness and interdependencies, recognize existing industry associations, and align to government agencies' roles and oversight responsibilities.[2]

[2] A Guide to Critical Infrastructure Security and Resilience, CISA

Identifying vital services, CI-s and CII-s

Setting an objective

'When identifying vital services, CI's and CII's it's important to consider many factors and to choose an appropriate approach which best fits the circumstance. It is important to remain focused upon the most critical services. Some services may not be critical to the functioning of society, or their interruption may not bring an immediate threat to people's lives, or interruptions to other vital services.

Many services that are provided by the State (for example, emergency communications, prisons, marine radio communications) have a higher level of resilience, as they may already be subject to annual work plans and have access to state budgets. Private companies may not have this, and so may be at more risk.'

Different practices of identifying vital services

In the European Union the Network and Information Security directive (NIS Directive EU 2016/1148[3]) sets out to enhance the level of cyber security effectiveness in critical service providers (or vital service providers across Member States. In 2019 a Report[4] was published which researched different methods used by Member States to identify and engage with critical service providers. In some countries a central approach was taken – a single authority was named to oversee all vital service providers in matters of cyber security, in others sectorial authorities were responsible for identification and supervision.

Another difference in approaches is if the identification is done in a top-down or bottom-up approach. In a top down approach an authority responsible for setting the thresholds and requirements identifies the vital service providers and notifies them of their status. This is a good approach if the number of vital service providers is manageable and their number is stable. A bottom-up approach is when the authority describes the thresholds for being a vital service provider and then each company in the sector must check if they meet the criteria, or not. The bottom-up approach works well if there are a large number of vital service providers and their number is in a constant change. In the case of a bottom-up approach it is seen as good practice that the vital service providers must inform the authority of their status and if they do not do it in a timely manner then sufficient penalties should apply.

There are many different approaches and methodologies. ENISA´s[5] guidelines also propose a concept of approach. Critical service-dependent approaches follow a three-step procedure. In this case, some countries first identify the critical sectors and then for each one of the critical sectors they proceed with the identification of critical services, critical applications and finally critical information infrastructure assets. In the following paragraphs, we detail each individual step.

[3] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546

[5] The European Union Agency for Cybersecurity

Step 1: Identification of critical sectors

Member States of the European Union have addressed the issue of identification of critical sectors to a greater or lesser extent and all have a longer or shorter **list of critical sectors,** which has been prepared taking into account national priorities, related EC Directives and specific country characteristics.

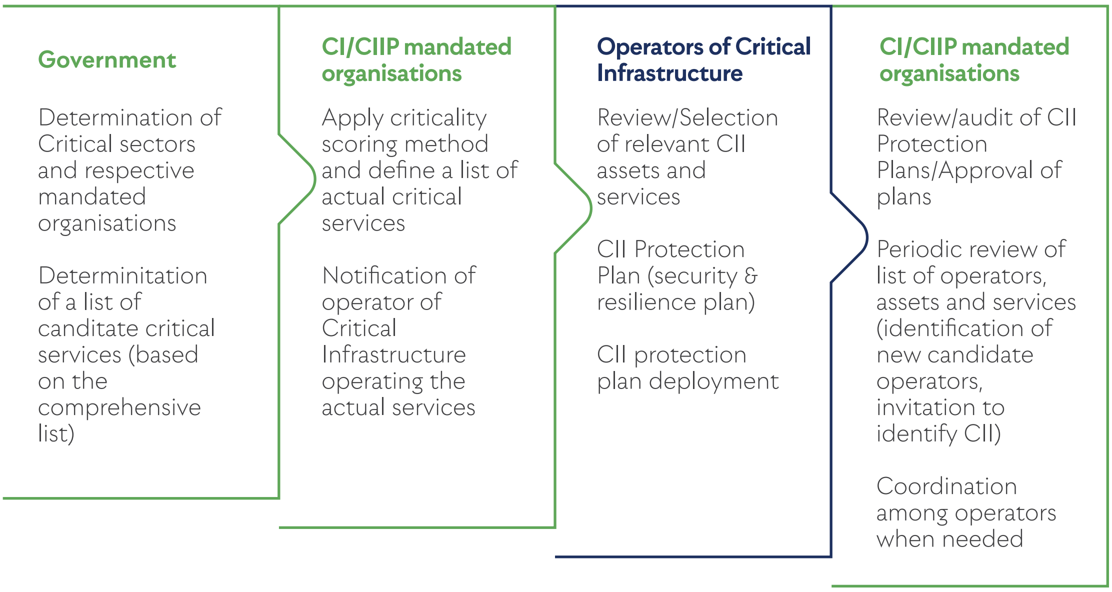
Step 2: Identification of critical services

Once the critical sectors are defined, the next step is to define the critical services such as for example water management, heating supply chains and public transport systems. At this point, we may differentiate between two approaches based on **who assumes the leading role for the identification of the critical services**:

a) the ***state-driven approach*** where the leading role is assumed by the government agencies that have the mandate to identify and protect CI - in most of the cases the responsible ministries.

In the case of the State-driven approach, the whole process is guided by the governmental agencies that have the mandate to identify and protect CIs. Having decided on the critical sectors, they apply a method to systematically identify critical services. Next, they identify the operators of CI involved in these services. The identification of specific assets may be performed in collaboration, aiming at assuring effectiveness, aligned with societal needs.

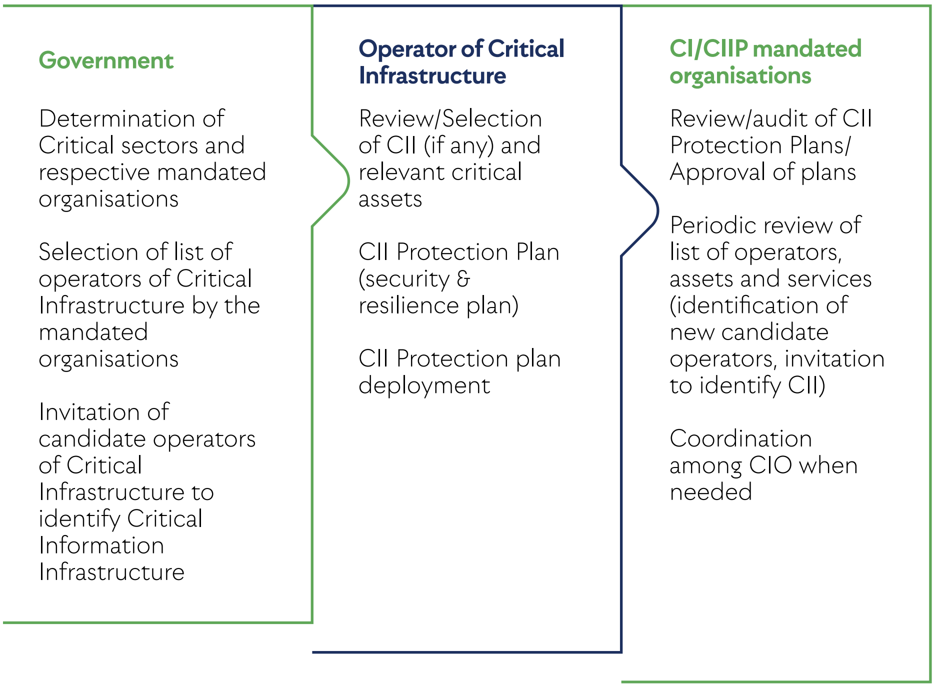
This approach and its steps are presented in the following table. Basically the CII/CIIP mandated organisations define the list of actual critical services and notify the operators of these services. The operator of CIIs is therefore in charge of defining the specific network assets and the appropriate measures that need to be taken to ensure the security and availability of connections. The mandated agencies then review the plan and periodically update the list of critical services due to continually changing threat landscape.



Government	CI/CIIP mandated organisations	Operators of Critical Infrastructure	CI/CIIP mandated organisations
Determination of Critical sectors and respective mandated organisations	Apply criticality scoring method and define a list of actual critical services	Review/Selection of relevant CII assets and services	Review/audit of CII Protection Plans/Approval of plans
Determinitation of a list of canditate critical services (based on the comprehensive list)	Notification of operator of Critical Infrastructure operating the actual services	CII Protection Plan (security & resilience plan)	Periodic review of list of operators, assets and services (identification of new candidate operators, invitation to identify CII)
		CII protection plan deployment	Coordination among operators when needed

b) the ***operator-driven approach*** where the leading role is assumed by the Critical Infrastructure Operators.

In the case of the operator-driven approach, the leading role is assigned to the operators of CIs. The country identifies a list of operators (called also 'vital operators'), who are responsible to identify the individual critical services and assets that comply with a number of risk analyses and risk management directives. Then, the responsible ministries review the selected services and assets along with the drafted CI protection plans.



Government

Determination of Critical sectors and respective mandated organisations

Selection of list of operators of Critical Infrastructure by the mandated organisations

Invitation of candidate operators of Critical Infrastructure to identify Critical Information Infrastructure

Operator of Critical Infrastructure

Review/Selection of CII (if any) and relevant critical assets

CII Protection Plan (security & resilience plan)

CII Protection plan deployment

CI/CIIP mandated organisations

Review/audit of CII Protection Plans/ Approval of plans

Periodic review of list of operators, assets and services (identification of new candidate operators, invitation to identify CII)

Coordination among CIO when needed

Step 3: Identification of critical information infrastructure network assets and services supporting critical services

Following the identification of critical services, the final step is to identify and classify the CII network assets and services supporting those critical services. This step represents the final phase of the translation of high level legislation into actual critical network assets and services that need to be secured, resilient and monitored.

These assets and services are part of a business supply chain. And as it was underlined at the beginning, due to their criticality, the associated business risk become national risks where the perimeter is now the business operations in provisioning that specific service.[6]

Estonia´s example

Estonia used the state-driven approach which was described in the previous chapter. For the selection of services also a methodology was adapted. The purpose of the methodology is to allow its users to objectively evaluate services from different aspects and the importance of services in comparison with each other and on this basis to determine which services are vital for the country. It is based on the Danish methodology for determining vital services and of the American and British experiences.

In Denmark vital services are evaluated by five categories: number of users, frequency of use, replacebility, importance for the functioning of other vital services, and time when the impact of interruption of the service appears. For

[6] Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks, ENISA

each category is a colour scale that goes from green to red (green – low impact, red – very important/critical).

Estonia considered it necessary to modify the Danish methodology. For each category certain criteria was developed which are the basis for the evaluation. Two new categories were added:

- timeframe of perceiving the consequences;
- influence on the life and health of the person in need of the service.

The modifications were made in order to make the methodology more transparent (it is equally understandable, which objective criteria are behind one number or colour) and easily justified by the parties.

The aim of both Denmark and Estonia's methodology is to assess whether or not the service, function or infrastructure is vital in the simplest possible way. The competence of the responsible ministry remains to determine which service providers are subject to the requirements of continuity. For example: the water supply services are vital but the requirements for continuity extend only to those water operators whose area of activity is the public water supply system which serves a residential area of 40 000 or more inhabitants.

Categories for determining the importance of services

Seven categories are used to assess the vitality of the services:

Methodology that Cyber4Dev recommends (Estonian example)

Categories for determining the importance of services
Seven categories are used to assess the vitality of the services:

1. **The number of users of the service –** the number of people who use the service within a year or are beneficiaries of the service. For example, in the case of marine pollution monitoring and control only the number of beneficiaries can be assessed not the number of users. The situation is similar to rescue service, weather forecasts, etc

2. **Frequency of use –** it was evaluated whether the service is often used by individuals or companies. Whether daily, regularly, randomly, by a specific target group etc

3. **Replaceability of the service –** it was assessed whether the service is replaceable or not. If the service is replaceable - the speed of replaceability and the equivalence of the alternative service;

4. **The impact of the service on other services –** it was assessed, how many services are affected by the interruption of the service and what impact the interruption will have;

5. **Is the service itself an alternative –** it was assessed whether the service itself can be used as an alternative service in the event of other service interruptions. For example: electricity can be used in households as an alternative to heating;

6. **The speed of arrival of the consequences –** the impact of the service interruption on users or services related to the service;

7. **The impact on the lives and health of people –** it was assessed whether the interruption of the service results by only discomforts or the interruption is fatal to the end user.

Scoring system

For each category it is possible to get points between -3 to 3. Where the category is divided into subcategories (categories 3 and 4) you can get between -1.5 to 1.5 points for the subcategory i.e. a total of -3 to 3 points for the whole category. Therefore, in all categories you can get a maximum of 21 points and a minimum of -21 points.

The services that are considered vital are those which receive at least 7 points in total and at the same time receive more than 0 points in category 4 and 7.

Identifying Vital Service Providers

Identifying potential authorities to manage Vital Service providers

COORDINATOR

ORGANISERS

SERVICE PROVIDERS

Coordinator

- Coordinates the fulfilment of responsibilities established in the relevant Emergency Act in their country (also supervising the organisers)
- Develops policy in order to ensure the continuous operation of vital services
- Advises agencies in organising the continuous operation of vital services

Organisers

- Establish requirements for the continuity of vital services. The requirements have to consider also the risk of interdependency of vital services.
- Approve the risk analysis and continuity plans of the service providers.
- Supervise the implementation of measures that prevent interruptions of vital services.
- Coordinate the resolution of an emergency that is caused by large-scale interruption of vital service(s). An emergency response plan is a cooperation agreement and it should include the following
    - who is authority in charge and who are participants,
    - what are their roles,
    - usable resources,
    - how information is exchanged, for example crisis communication for the public etc.
- Manage risk communication – to raise public awareness and increase readiness for emergencies. The organiser should notify the public of threats that could interrupt the vital service and could lead to an emergency.
- Deliver regular exercises – 1 exercise every 2 years to test the emergency response plan and all parties should be included. Exercises are also important for the vital service providers.

Service providers

- Preparing a continuity risk assessment and plan of the provided vital services
- Improving preparedness for crisis situations
- Arranging exercises to test their plan
- Ensuring continuity of the vital services

Description and continuity requirements

Continuity requirements establish a framework for the continuity of vital services and lay down the list of vital service providers. It is important to describe the availability level of vital services and service provision readiness, as well as measures for the prevention of interruptions to vital services. This also includes the procedure for the restoration of vital services and circumstances amounting to an emergency caused by an extensive or severe interruption to a vital service, as well as the procedure for reporting an emergency or a threat of emergency.

Example (finance sector)

1) In case of an emergency, the service provider shall ensure that:
    1. at least 10% of cash distribution points remain operative;
    2. payments between the accounts opened with the service provider and those with other service providers are settled at least once per settlement day;

2) A vital service is interrupted if due to failures in the delivery of the service, the number of service transactions falls below 20% of the average number of transactions for a comparable preceding period.

3) The maximum permissible duration of an interruption to a vital service shall be 12 hours.

Proposing criteria and thresholds for identifying critical service providers

A first selection of CI and CI services within a sector can be made based on sector-specific criteria. Such criteria may be the market share, the transport capacity, cross-border connectivity (import and/or export), supply of critical services to government, industry or population.

This first step results in a CI short-list from within a particular sector. This step also narrows down the number of potential CI operators in the case where the sector has multiple operators. Be aware that sector-specific criteria may be treated as classified information by some nations as they could reveal dependencies, vulnerabilities and sensitivities. This leads to a short-list of CI from which further deliberations are to be made.

Are all CI-s CII-s?

Not all services that are identified as part of the CI of a country contain a CII component. Some services have a clear CII dependency for example telecommunication services and other services may also function without a CII component.

For the proper functioning of a country it is important to identify and classify the CII network assets and services supporting those critical services. This step represents the final phase of the translation of high level legislation into actual critical network assets and services that need to be secured, resilient and monitored.[7]

[7] Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks, ENISA

Political process to agree: development of legislation

- Preparing and implementing a CIIP framework requires significant involvement of the public and private sector. It requires dedicated financial resources and participation of academia. A significant level of engagement can be achieved by high prioritization of the CIIP agenda at the national level through primary countrywide strategies, such as a national security strategy.
- Clear Governance Model for CIIP governance at the national level should not be complex. There should be one or only a few policymaking bodies involved at the national level, with clear assignment of sectoral coordination down the line.
- Each critical infrastructure sector should have its own governance structure that monitors implementation of sector-specific CIIP measures, and coordinates and strengthens collaboration among critical infrastructure owners and operators.

Critical Information Infrastructure Protection

Legal requirements for Vital Service providers

When designing requirements for vital service providers, it is a good idea to keep the general principles in a law at the highest legislative level and more detailed requirements at a regulation level. It is best to go for the accepted practices in your county as several sectors that presumably have vital service providers have other laws and regulations that they must follow.

In cases where the detailed requirements are specified by law, it may be cumbersome to keep them up to date and it is important to change the detailed requirements as the cyber threat landscape evolves. Otherwise, if the requirements contain long-time obsolete requirements, the vital service providers could take the requirements as a something to be done for compliance and not for actual benefit for security.

Some countries have detailed requirements for vital service providers. These are typically countries with very mature and capable government agencies, who have the opportunity to maintain a high level of technical competence in very specific fields - for example cyber security of electrical substation industrial control systems. For smaller countries or countries with different approaches to supervision and regulation of sectors, it can be difficult or nearly impossible to keep that level of expertise 'in house'. For them a good approach is the risk-based approach, where in co-operation with the service providers the risks are evaluated and proper measures are taken to mitigate or lower the risks to acceptable levels. This approach gives more flexibility, but it would be more difficult to have a confirmed base level of security in the sector.

An example of different risks would be two water utility companies. Let's say that they both have approximately 40,000 customers and the same level of digitalisation.

Company A clients are all in one town, closely together. Company A uses surface water that is chemically treated to purify the water and has one big water treatment plant.

Company B has 20 different rural areas where they provide drinking water. All sites have independent groundwater wells and no chemical purification is needed for the water. In addition, large proportion of their clients still have access to their own wells.

The two companies have the same number of clients, but the **impact** on their customers is very much different if they have a disruption in their service.

Supporting Vital Service providers

In addition to setting legal requirements and supervising the compliance with set requirements, it is essential to support vital service providers in implementing organisational and technological measures, as well as training personnel.

Companies in general are eager to be more secure, but there is a gap between legal requirements and gaining an understanding of what needs to be done in practice. Furthermore, vital service providers (IT) organisations can vary vastly between the service providers, so implementing a security measure in one company may be a simple task of reconfiguring existing systems, whereas for another company it may be necessary to start with the recruitment of additional personnel, rebuilding networks and buying extra hardware.

Another way of providing support on implementing requirements is through training. Staff training is a great opportunity for service providers to gain an insight into the true level of cyber security knowledge within their company, that would otherwise be hard to attain.

Another aspect in providing support for implementing requirements is the fact that while trainings and sharing information, the organisers of vital service can get a good insight of the level of cyber security in a company, that would be otherwise hard to attain. It is always possible to go through official supervisory process but people are generally more forthcoming in unofficial setting.

Networking and information sharing

One of the most important measures that a vital service provider can facilitate is **information sharing.** Cyber criminals are people, so in general they reuse successful attacks as much as possible, so they don't have to do extra work! And they are successful in large part, since victims of successful attacks tend to not talk about the fact that they were attacked and how it happened. This is where the organiser of vital services can encourage and establish information sharing groups and channels to help service providers to discuss their cyber incidents and other topics related to cybersecurity.

Practice shows that it is optimal to organise information sharing get-togethers by sector. In a sector, challenges and solutions are similar and people know each other at some level. Sectorial get-togethers have loose agendas and it is a good idea to rotate the place of attendance between the members, so that the group has joint ownership of the discussion.

At get-togethers, topics are proposed by the members and usually involve an overview of the notable topics from the host, followed by presentations and discussions from the group members. They may discuss recent incidents, implementing security tools and describe why they chose this tool and what the relative pros and cons after using a tool for a while are.

As information is only shared with those who are trusted, it is a good idea to agree on the rules of the information sharing. A good starting point would be to apply the Chatham House Rule[8]:

> "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

Also, emphasising that vital service providers are generally not competitors in the security field, it is important to recognise that for them their public reputation may be far more important than the security posture of a single company. For example, if a e-banking solution of 'Bank A' is unsecured, then every bank needs to start proving that their solution is secured. So, it might be rational for the banking sector to work together on security issues.

Tools

Several modern security tools and capabilities can be provided or at least recommended centrally. To implement these tools effectively, organisations need to have trained personnel and hardware recourses available; and for many smaller vital service providers it can be a challenge to implement them in a useful manner. Working together with a national CERT or other similar organisations can be useful as they can provide tools and services

[8] The Chatham House Rule https://www.chathamhouse.org/about-us/chatham-house-rule

such as manual and automated malware analysis, cyber forensics, network monitoring solutions, secure DNS etc. Although there are public alternatives for many of tehse tools and services, it is wise to analyse what happens with the data uploaded to those public services.

A good example of a tool provided centrally is **CERT-EEs Cuckoo Sandbox**[9]- an automated malware analysis sandbox that can be used to determine if a suspicious file is malicious and what it tries to do if executed. Similarly popular amongst CERT-EE clients is the **Suricata4all (S4A) IDS system**[10]**. S4A is a distributed intrusion detection system (IDS).** It utilises open-source software components to monitor, analyse and capture network traffic to detect possible intrusions.

These and other central tools also give insight and better situational awareness of the cyberspace for the CERT teams as well as the vital service provider.

Frameworks, standards and guidelines

There are many frameworks and guidelines available for cyber security. Some are general, others have a more specific sector in mind. It can be challenging for the vital service provider to select an optimal framework, standard or guideline to implement. NIST[11] and ISO[12] families are the most well-known but it may be a good idea to have a national standard as well or to start out with best practice guidelines like CIS Critical Security Controls[13].

It is up to the organiser of the vital service to set the rules of which framework, standard or guideline must be followed by the vital service provider.

Training

One of the core starting points for assuring cyber security is conducting a thorough risk assessment. For many organisations, this may be their first experience of formally assessing risks and especially IT risks. IT risk assessment training can be one of more popular training that the organizer of the vital service can provide for the vital service provider. Amongst others are specific trainings on network security, forensics, tools and services provided by to the vital service providers. Generally, trainings that do not have publicly available offerings or assembling a study group and procuring the training centrally with noticeable savings are good candidates for the organizer of the vital service to offer.

Exercises

Cyber exercises play a big part in developing a wider resilience amongst vital service providers. There are several cross-dependencies between vital service providers – the most obvious is that telecommunication requires electricity to provide the service and power generation; and distribution presumably needs telecommunication to manage their grid. When a wide scale incident occurs in one of the vital service providers, it is necessary to coordinate responses and mitigation measures amongst connected service providers and perhaps at a national level as well. To streamline this process and avoid problems, gaps and overlaps on cyber

[9] Available at https://cuckoo.cert.ee/

[10] Suricata4All Github at https://github.com/cert-ee/s4a

[11] https://www.nist.gov/cyberframework

[12] https://en.wikipedia.org/wiki/ISO/IEC_27000-series

[13] https://www.cisecurity.org/

crisis management, cyber exercises should be conducted.

There are several types of exercises to choose from. Perhaps the simplest one to organise is a table top exercise within a vital service provider to practice and test their internal procedures. A table top exercise is relatively cheap to arrange and does not demand a lot of time from the participants. Furthermore, more generic scenarios can be constructed and reused with small modifications in several vital service providers in a sector.

There are several resources available that can be useful in choosing the scope and type of exercise. European Union Agency for Cybersecurity (ENISA) has published a "National Exercise - Good Practice Guide"[14] some time ago and more recently Finnish Transport and Communications Agency (TRAFICOM) published a "Instructions for organising cyber exercises – A manual for cyber exercise organisers"[15]. Both give a good overview of what to take in account when organizing cyber exercises.

Supervision

An essential tool in ensuring the long-term effectiveness of CIIP is supervision.

Hopefully, at this point, there is no doubt about the importance of information security measures. In today's world, every organisation is required to understand how information security helps to keep their business running and customers happy. This means implementing security measures in accordance with the regulatory framework in the countries in which they operate. In Estonia, it is mainly the Cyber Security Act, together with its predecessors and related acts.

Even when the requirements set out in legislation are fulfilled by the company, it's essential that the organisation continues to maintain these standards. There may come a time when the implementation of the measures need to be validated, to check whether information security measures are being implemented fully. For this purpose, there is a supervisory function.

What is supervision? Depending on the topic and area, it can mean different things. In our context and for this purpose, we define supervision as the following:

Supervision is a complex set of legal, technical and analytical activities and procedures, conducted by a mandated entity in order to verify the compliance with applicable requirements and, if necessary, force the subjects to comply with the requirements.

As we look at the role of supervision, we see that it is made up of different activities and procedures and together they form a sophisticated mechanism which is designed to ensure that there are sufficient checks and balances in place to assess whether an organisation is implementing CIIP measures correctly. The mandated entity carrying out supervision must have a mandate to do so by law, to ensure the legitimacy of this function. The goal of effective supervision is to check that the necessary security measures, guided by law, are in place. And if that is not the case, a supervisory function has the power and obligation to force the subjects of the law to comply with the rules.

Who are the subjects? According to the Estonian Cyber Security Act, all of the following organisations are subjects of that law and therefore also subjects to supervision, carried out under this law. The subjects are

[14] https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide

[15] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf

- Governmental organisations
- Local government organisations
- Vital service providers
- Telecom service providers
- Digital service providers
- Health service providers
- Trust service providers
- Members of X-road

There are some overlaps in these groups, for example some of the telecommunication and trust service providers are also part of the vital service providers' group. Altogether there are currently about 400 main subjects in Estonia, but if we also include groups that are likely to fall under the Cyber Security Act in the future, then the number goes rapidly to circa 2000 organisations.

What does a typical supervision project look like? As it is an official procedure, it has to have the necessary formalities, including an initiation letter that is sent out to inform the subject about the upcoming supervision. This letter must contain the legal grounding and details of the mandate to perform the supervision, a general description of the reason for the inspection and any possible concerns, as well as the request of the initial documents and evidence.

The subject must comply with this request as it is mandated within the law. Once the subject supplies the materials and evidence, they are analysed and from this, the team carrying out the supervision can assess whether the organisation does indeed follow their own mandated policies in real life scenarios. From this, a preliminary assessment or a working hypothesis is created. After that, various on-site activities are conducted.

These include:

- Interviews and/or interrogations with the subjects' representatives. It is important to conduct interviews with executive level members, as it is within the C-Suite where the overall responsibility lies. In addition to that, interviews with other key-figures of an organisation are conducted.
- On-site activities also include checks on the physical infrastructure, such as buildings, their locks, cabling, fire extinguishing readiness, server rooms, surveillance systems etc. Supervisory officials can ask for a demonstration of how restrictions work in real life (admin accounts for standard users etc). If necessary, vulnerability scans and/or penetration tests are conducted.
- After on-site activities are conducted, all the information that has been collected is analysed by the supervision team and conclusions are presented to the organisation which has been assessed. The supervised organisation always has the right to explain and express their opinion about any possible shortcomings that are found and this is taken into consideration in the final verdict / conclusion of the supervisory inspection.

Minor problems are usually fixed during the supervisory process, but for bigger shortcomings more time is needed and sometimes an action-plan to address the these will be negotiated. It is important that the supervised organisation is given an opportunity to resolve their shortcomings and lift their performance before sanctioning. If they do this in a reasonable period of time and a reassessment proves that they have made sufficient improvements, then the case for sanctioning would be closed. If they fail to make the required improvements, then they must provide a satisfactory justification for this. If the explanation doesn't satisfy the supervisory official, a sanction will be imposed. In a public sector organisation, this would typically be a compulsory order that obliges the subject to have their security shortcomings fixed by a given, reasonable deadline. After the deadline, a follow-up check is made in order to verify it. In a private sector organisation, a reoccurring monetary fine may follow. This type of fine will be imposed repeatedly, until the problem is fixed.

Sanctioning is never the objective of a supervision. The main aim is to ensure that any problems are quickly fixed. Sanctioning is the last resort, if all else fails. Therefore, supervisory officials always take time to explain things in order to reach a constructive consensus. At times, a consultative supervision and capacity building activity can be offered, if it is deemed to be more effective than punishment; and if it does not infringe on the objectivity of the subject. In this instance, it is important to note that this can be done only on a general level and in a limited quantity, as otherwise, if the supervisory officials provide in detail consultancy, there would be a conflict of interest regarding the objectivity of further supervisory proceedings.

As supervision is an administrative procedure, it also ends with an administrative act (decision) and instruction. If the supervised organisation believes that that the supervisory official has been unjust towards them or they simply do not agree with the decision, they can challenge the decision in the administrative court. However, since the introduction of the supervisory function in cyber security in Estonia (circa 10 years) not a single decision has ended up in the court.

Supervision is an important function that makes a valuable contribution to cybersecurity. Many states and organisations are nervous about the idea of supervision and assessment, however it has proven to be an essential activity which can be conducted in a constructive way, while still delivering results and ultimately an improved level of protection against cyber threats.

Testimonials: CIIP activities delivered by Cyber4Dev

The Gambia

Cyber4Dev recently trained over 60 personnel from potential Critical Information Infrastructure (CII) entities in The Gambia. The training provided participants with information on the fundamentals of critical infrastructure and information on how to identify and categorise correctly. The Cyber4Dev Training, on such a grand scale, was one of a kind for The Gambia. This has led to an agreement with the Ministry of Information and Communication Infrastructure to constitute a National Critical Information Infrastructure Committee (NCIIC) to work together in formulating a NCII Policy for The Gambia.

Many Thanks to Cyber4Dev, OCWAR-C, ECOWAS and the Estonian Government.

Representative from The Gambian Government

Guyana

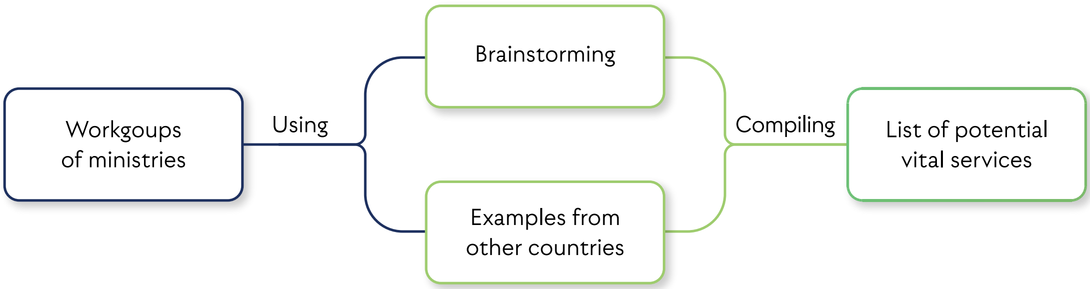
During the period February – July 2021, the Cyber4Dev project provided technical assistance which concluded with a proposal for the development of a national Critical Information Infrastructure Protection (CIIP) framework in Guyana. Cyber4Dev hosted training sessions and facilitated stakeholder workshops with representatives from key sectors which led to the identification of critical services, and critical information infrastructure across Guyana. I am appreciative of this initiative and the understanding of the next steps required for Guyana to develop its CIIP framework.

Manager - Cybersecurity
National Data Management Authority

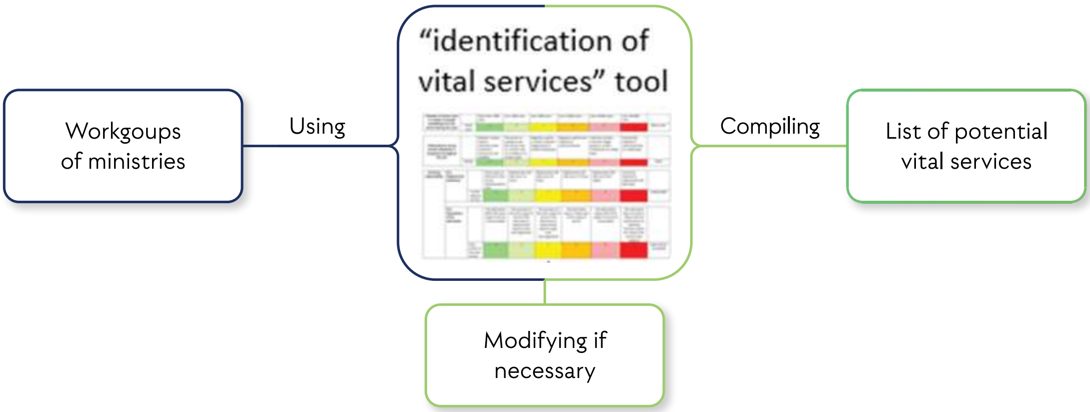
Appendix:
Excel based tool

Example Figures

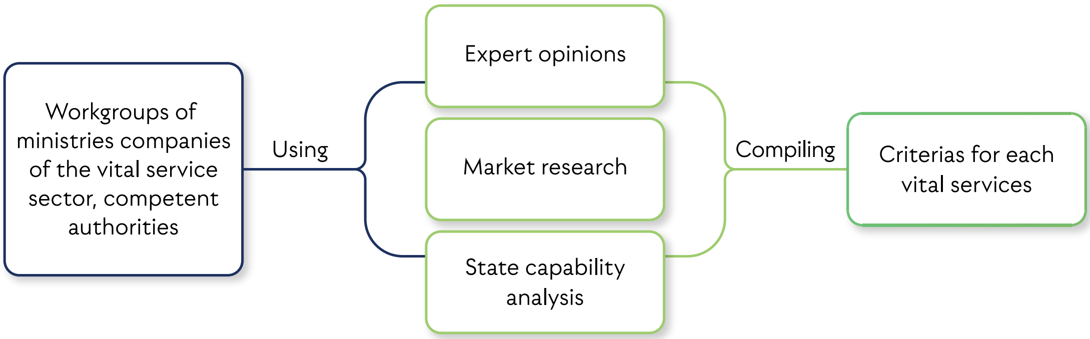
Step 1: Compiling a list of potential vital services


Workgoups of ministries
Using
Brainstorming
Examples from other countries
Compiling
List of potential vital services

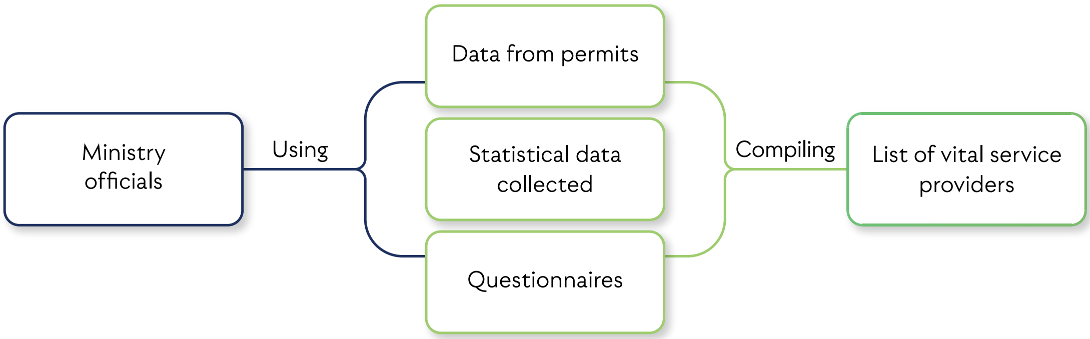
Step 2: Verifying the potential list of vital services with the “identification of vital services” tool


Workgoups of ministries
Using
“identification of vital services” tool
Compiling
List of potential vital services
Modifying if necessary

Step 3: Specifying criteria for companies to become vital sevices providers


Workgroups of ministries companies of the vital service sector, competent authorities
Using
Expert opinions
Market research
State capability analysis
Compiling
Criterias for each vital services

Step 4: Identifying companies that are vital service providers



CYBER4Dev

www.cyber4dev.eu

Funded by the
European Union