



About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Cédric Lévy-Bencheton (ENISA), **Dr. Louis Marinou** (ENISA), **Rossella Mattioli** (ENISA), **Dr. Thomas King** (DE-CIX Management GmbH), **Christoph Dietzel** (DE-CIX Management GmbH), **Jan Stumpf** (DE-CIX Management GmbH)

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu

Acknowledgements

For the completion of this study, ENISA has worked closely with:

- The "Internet infrastructure security and resilience" reference group.
- Individual experts that reviewed the results and provided valuable feedback: **Randy Bush** (Internet Initiative Japan), **Patrick Fältström** (Netnod), **Peter Koch** (DENIC), **Benno Overeinder** (NLnetLabs), **Andrei Robachevsky** (Internet Society).

We are grateful for their valuable input and comments.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

© European Union Agency for Network and Information Security (ENISA), 2014

Reproduction is authorised provided the source is acknowledged.

Catalogue number: TP-05-14-012-EN-N

ISBN: 978-92-9204-098-7

DOI: 10.2824/34387

Executive summary

The Internet infrastructure supports the global exchange of information through physical and logical assets, such as cables, servers, protocols, services... These assets suffer from various threats that can hamper network connectivity and disrupt the Internet.

As a threat landscape, this study gives a detailed overview of the current threats applicable to the Internet infrastructure and their trends, so that Internet infrastructure owners can improve their security using good practices.

For that purpose, this study details the assets of Internet infrastructure (structured into eight types: hardware, software, information, human resources, protocols, services, interconnections, and infrastructure) and list the threats applicable to these Internet infrastructure assets. These results are structured into mind maps. The study then classifies Important Specific Threats of the Internet infrastructure – namely Routing threats, DNS threats, Denial of Service, and Generic threats – and links each threat with a list of assets exposed.

As a good practice guide, this study details a list of good practices that aim at securing an Internet infrastructure asset from Important Specific Threats. A gap analysis identifies that some assets remain not covered by current good practices: human resources (administrators and operators) for Routing, DNS and Denial of Service, as well as System Configuration and Essential Addressing Protocols for Denial of Service.

This study provides Internet Infrastructure owners with a guide to assess threats applicable to their assets. It proposes recommendations to improve the security of the Internet infrastructure. These recommendations are sorted into:

Five technical recommendations:

- Recommendation 1: For Internet Infrastructure owners and electronic communications network regulatory agencies, evaluate your current level of security by understanding the assets covered (and not covered) by existing security measures.
- Recommendation 2: For Internet infrastructure owners, evaluate the application of adapted good practices in a focused manner.
- Recommendation 3: For Internet infrastructure owners, cooperate with the community to exchange on threats and promote the application of good practices as mitigation measures.
- Recommendation 4: For users deploying good practices guides, report on their implementations, assets covered and gaps found.
- Recommendation 5: Words matter: Ensure the right use of terms and definitions.

And four organisational recommendations:

- Recommendation 6: For Internet infrastructure owners, use proper risk assessment methods to understand vulnerable assets in your Internet infrastructure and prioritise your protection actions.
- Recommendation 7: Build an information and communication technology security awareness and training program.
- Recommendation 8: Internet infrastructure owners shall commit third-party vendors to apply security measures.
- Recommendation 9: Internet infrastructure owners should stay current on any updates.

Table of Contents

Executive summary	iii
1 Introduction	1
1.1 Policy Context	1
1.2 Target Audience	2
1.3 Scope of the Study	2
1.4 Structure of this Study.....	3
2 Methodology.....	4
3 Internet Infrastructure Assets	5
4 Threats of the Internet Infrastructure	7
4.1 Threat types	7
4.2 Important Specific Threats of the Internet Infrastructure.....	10
4.2.1 Routing Threats	10
4.2.2 DNS Threats.....	12
4.2.3 Denial of Service (DoS/Distributed DoS (DDoS)) Threats	14
4.2.4 Generic Threats	16
4.3 Summary of threat trends	17
5 Internet Infrastructure Assets Exposure to Cyber Threats.....	19
6 Threat Agents	21
7 Good Practices.....	22
7.1 Gap Analysis.....	26
8 Recommendations.....	28
8.1 Technical Recommendations.....	28
8.2 Organisational Recommendations	31
9 Conclusion.....	33

1 Introduction

The Internet, as a network of independent computer networks, has grown into an important global platform of commercial and private interest as well as for e-government and public services for our society, thus making up an indispensable utility for all areas of life. As a complex system, it largely depends on different components, mechanisms and functions on various levels of abstraction. The infrastructure of the Internet, as the underlying base, comprises of hardware, physical infrastructure, interconnection, software, protocols, information, services, and human resources. For instance, networks (autonomous systems) are connected by components of the physical layers, but they are addressed by logical addressing schemes, carrying data via a set of protocols to the desired destination, and operators who can leap into action when trouble occurs. A failure of those core components does not only cause a disruption of a network or some participants, but it may also influence a large portion of the Internet, up to its entirety.

This *Threat Landscape and Good Practice Guide for Internet Infrastructure* (IITL) is one of the deliverables (Work Package 1.1 – Deliverable 2) foreseen in the ENISA Work Programme 2014 under the Work Stream ‘Support EU policy building’.¹ It provides an overview of the current state of cyber security in this domain.

This study is intended to enhance guidance available on the security of the Internet infrastructure. By doing so, it starts off with taking stock of assets which can be found at Internet infrastructure operators such as Internet Service Providers (ISP), Internet Exchange Points (IXP), or other network carriers. Based on assets identified, this study carries out a threat assessment by taking into account the specifics of the Internet infrastructure and moreover provides a starting point to support further risk assessments. Those threats are termed as important specific threats for the Internet infrastructure. Assets and threats are brought together to identify the most important exposures. Originators of threats, i.e. the threat agents, are classified, described, and mapped to the previously identified threats. They are taken further into account in order to develop a list of existing measures such as good practices that aim to reduce the asset’s attack surfaces. Following this, assets not covered are identified and reasons are given for the lack of protection measures. Finally, the experience gained during this study is joined with the feedback of the experts who were consulted to draw a conclusion and summarise technical as well as operational recommendations to support the protection of the Internet infrastructure and the security of networks.

This study, and notably the recommendations, have been agreed upon with experts from the ENISA Internet Infrastructure Security and Resilience Reference Group. Due to the assessment performed and the valuable feedback of experts, this study covers the most important building blocks of the Internet infrastructure. However, one must be aware that such a study cannot be exhaustive, due to dynamics of the infrastructure in at stake and the threat environment.

1.1 Policy Context

The Cyber Security Strategy for the EU² stresses the importance of threat analysis and emerging trends in cyber security. The ENISA Threat Landscape is an activity towards achieving objectives formulated in this regulation, in particular by contributing to identifying emerging trends in cyber-

¹ “ENISA Work Programme 2014”, <http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014>, in particular, p. 16.

² <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>

threats and understanding the evolution of cyber-crime (see ENISA's *Understanding the Importance of the Internet Infrastructure in Europe*).³

Moreover, the new ENISA regulation⁴ mentions the necessity to analyse current and emerging risks (and their components), stating: "the Agency, in cooperation with Member States and, as appropriate, with statistical bodies and others, collects relevant information". In particular, under Art. 3, Tasks, d), iii), the new ENISA regulation states that ENISA should "enable effective responses to current and emerging network and information security risks and threats".

From the above-mentioned reasons, it becomes apparent that the ENISA Threat Landscape is a significant contribution to the EU Cyber Security Strategy, streamlining and consolidating available information on cyber-threats and their evolution.

This study aims to provide a significant contribution towards assessing the cyber threat exposure of the Internet infrastructure. As such, it will directly contribute to the assessment of cyber security as well as supporting investor and industry concerns.

1.2 Target Audience

This material is a tool for Internet infrastructure asset owners who, based on this study, wish to perform detailed threat analyses and risk assessments according to their particular needs/scope (i.e. asset protection level based on asset impact, vulnerabilities and detail of mitigation measures). In this study the threat exposure of Internet infrastructure assets is being presented; asset owners may deepen their threat analysis and risk assessment by using the asset and threat details provided. A deeper analysis by the asset owners should be based on assessed threats, vulnerabilities, and impact statements with regard to the concrete assets deployed by the Internet infrastructure operators.

Moreover, policy makers can rely on the Internet infrastructure threat landscape to understand the current state of threats, trends and associated mitigation measures. Such threat landscape may constitute an input to develop policy actions in the areas of cyber security, critical infrastructure protection and Internet infrastructure in particular.

Through the significant number of reports collected, the Internet infrastructure threat landscape provides a unique collection of information regarding cyber security threats. Hence, a further target group of this study are individuals who would like to obtain access to these sources in order to use them for their own purposes.

1.3 Scope of the Study

The definition of the Internet used throughout this study is similar to the definition employed by RFC 2026:⁵

The Internet, a loosely-organized international collaboration of autonomous, interconnected networks, supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards. There are also many isolated interconnected networks, which are not connected to the global Internet but use the Internet Standards.

³ ENISA, "Understanding the Importance of the Internet Infrastructure in Europe", <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/guidelines-for-enhancing-the-resilience-of-ecomunication-networks>

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF>

⁵ RFC 2026, <http://www.ietf.org/rfc/rfc2026.txt>

Based on this definition, the Internet Infrastructure consists of a wide range of assets residing on different physical and logical layers, which are crucial for its proper operation. The scope of this study focuses on the threats applicable to these physical and logical assets, as presented in Figure 1.

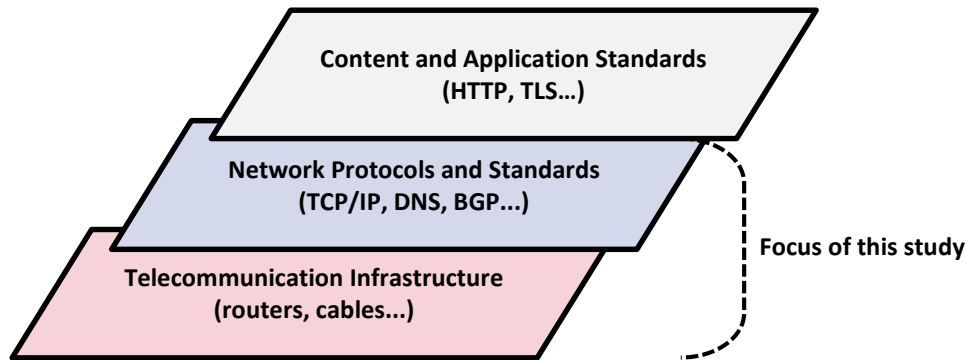


Figure 1 – Focus of the Threat Landscape and Good Practice Guide for Internet Infrastructure

This study proposes a threat landscape, which is an overview of current threats applicable to the Internet Infrastructure and their associated trends. The goal is to enhance the security of the Internet Infrastructure by detailing a list of good practices and recommendations for important specific threats.

1.4 Structure of this Study

The remainder of this study is organised as follows:

Chapter 2 gives insight into the methodology followed during the execution of this study.

Chapter 3 presents all relevant Internet infrastructure asset types. An overview of the assets and their dependencies is depicted in a mind map.

Chapter 4 elaborates on the threat types that the previously defined assets are exposed to. The developed taxonomy is presented as mind map and the most relevant threats are clustered into important specific threat groups and their trends are indicated.

Chapter 5 deals with the exposure of the identified assets to cyber threats.

Chapter 6 introduces the threat agents and maps them in regard with the threat types.

Chapter 7 lists and summarises available Internet infrastructure security measures mitigating the important specific threats. Assets which are not covered are identified and the reasons are outlined.

Chapter 8 builds on lessons learned during the study and summarises experiences gained in technical and organisational recommendations.

Chapter 9 concludes.

All material that is referenced by a URL in the footnotes is available on the day of publication of this study. It is also worth mentioning that in order to keep the size of this study manageable, detailed material is provided by means of annexes. These shall support Internet infrastructure asset owners to perform a risk assessment.

2 Methodology

The methodology followed in this study is similar to the methodology introduced by the ENISA Threat Landscape 2013.⁶

In order to identify required protection levels for valuable assets it is common to perform a risk assessment. Subsequently, security measures have to be introduced to achieve assessed protection levels by mitigating (part of) the assessed risks. Other risks might be transferred or accepted. As discussed below, threats are an important element in risk assessment.

In this section, the methodology followed in the IITL is presented. It consists of a number of threats to which the Internet Infrastructure assets are exposed. Hence, the presented IITL is an important tool for those who want to assess the risks within an IT environment of any complexity. Based on these risks, appropriate security measures can be selected to achieve risk mitigation. Identified good practices can be used as a guideline for achieving this goal.

The role of threats in the risk assessment equations becomes evident when looking at the components of risks. According to the widely accepted ISO 27005 definition, risks emerge when: *“Threats abuse vulnerabilities of assets to generate harm for the organization”*. In more detailed terms, the risk is considered as taking into account the following elements:

Asset (Vulnerabilities, Controls), **Threat** (Threat Agent Profile, Likelihood) and **Impact**

This study does not assume the use of any particular Internet or network infrastructure equipment or the operational processes or services. As such, it is impossible to make any valid assumptions about impact and vulnerabilities of assets. These are activities that can solely be performed by the asset owner. Hence, the need for supporting tools for the performance of risk assessments becomes obvious and essential for the asset owner in this complex environment.

The elements of risks are graphically depicted in Figure 2 below:

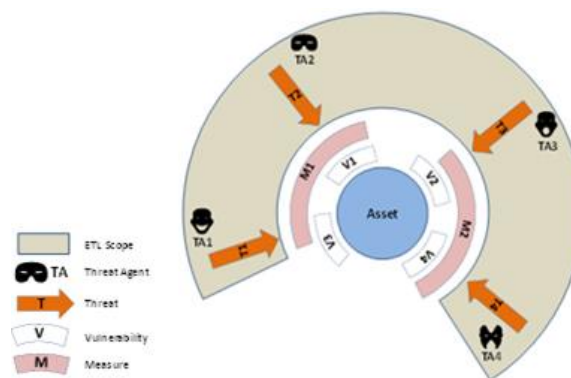


Figure 2– Threats targeting an asset by trying to exploit its vulnerabilities

This figure has been adopted from ISO 13335-4 and shows how threat agents (cf. Chapter 6), deploying threats (T), try to exploit asset vulnerabilities (V) in order to harm/take over the asset. The asset owner has implemented security measures (M) to protect the asset, that is, to eliminate or significantly reduce its vulnerabilities. The impact achieved by the potential materialization of a threat is the final element to evaluate the risk of an asset (see also risk definition above).

⁶ “ENISA Threat Landscape 2013”, <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats>

3 Internet Infrastructure Assets

According to ENISA’s *Guideline on Threats and Assets*⁷ published in the context of ENISA’s *Security framework for Article 4 and 13a*⁸ proposal, an asset is defined as “... anything of value. Assets can be abstract assets (like processes or reputation), virtual assets (for instance, data), physical assets (cables, a piece of equipment), human resources, money”. Nevertheless, for information security considerations this study focuses on assets that are mainly related to information and communication technology (ICT) under the scope of the Internet infrastructure.

Assets of the Internet infrastructure ensure the connectivity of networks from a physical and logical point of view. An asset taxonomy is presented to structure all relevant assets, illustrated in Figure 3. Due to the complexity of the Internet infrastructure the assets are grouped into asset types of different granularity and scope. For instance, the operation of a router requires the hardware which can be found at a physical location, a configuration, software that instantiates the configuration, essential addressing services for interconnection defined by a set of protocols, and an operator to monitor its current state. Hence, the granularity of asset types, even if they are arranged on the same level of the taxonomy, may vary. In addition to the ICT assets, several non-IT assets are identified. They strongly depend on ICT and are central for the proper operation of the Internet. For instance, buildings, power supply, cooling systems, or human resources. A detailed description of these assets is given in Annex A.

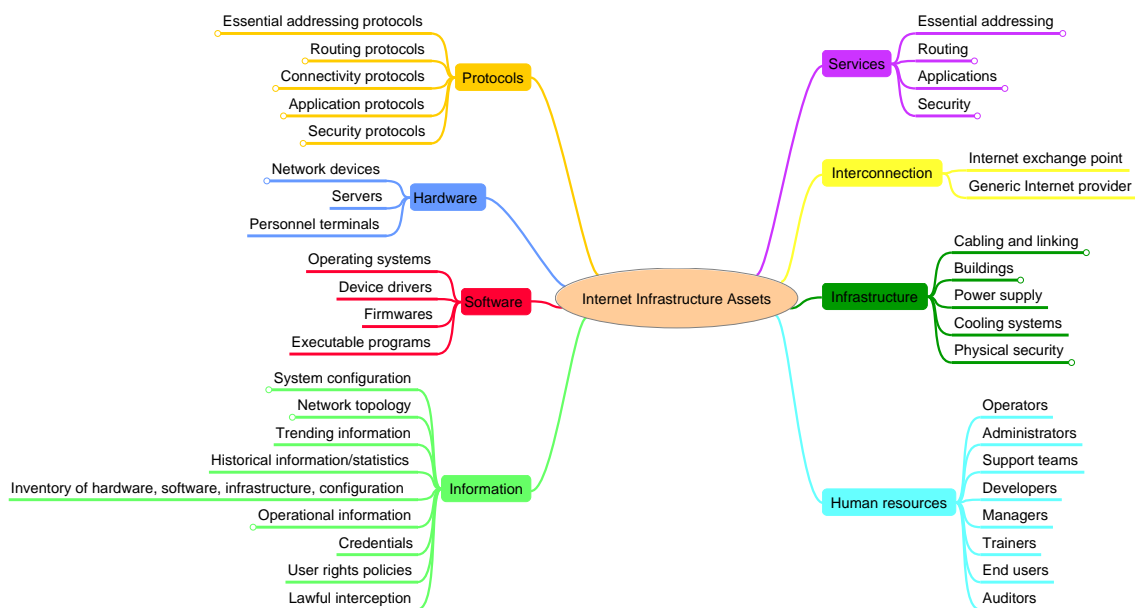


Figure 3 – Assets of the Internet infrastructure (levels 1 and 2 - see Annex B for the expanded mind map)

The mind map presented in Figure 3 gives an overview of all assets determined and is structured into asset types according to their use. However, an asset is not necessarily an exclusive member of just one asset type. For readability, the details of the mind map are limited to the secondary level. An expanded version is presented in Annex B. In the following the asset types are presented for the first level of the mind map:

⁷ https://resilience.enisa.europa.eu/article-13/guideline-on-threats-and-assets/guideline-on-threats-and-assets/at_download/file

⁸ http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security-framework-for-articles-4-and-13a/at_download/fullReport

The asset types **hardware**, **software**, **information**, and **human resources** comprise the same assets as in former studies^{7 10} and can be thought of as intuitively clear. Moreover, the following are particularly applicable to the Internet infrastructure:

- A **protocol** is a set of digital rules for data exchange within or between computer systems. Protocols are valuable assets for the Internet infrastructure because they allow meaningful communication between different computer systems.
- A **service**, with regards to the Internet infrastructure, refers to an abstract combination of other functionalities utilizing other assets in order to fulfil a defined task. Services are important, as the Internet is built around services.
- **Interconnection** covers the organisations building and running large computer networks. As the Internet is a network of different large computer networks, the assets providing interconnection functionality are very valuable.
- The term **infrastructure** denotes the basic physical structures and facilities (e.g., buildings and cables) needed for the operation of the Internet. In order to build a worldwide network of networks, the so-called Internet, the supporting infrastructure is crucial.

The asset taxonomy presented should only be considered as a snapshot of the complex range of Internet assets and can as such not be exhaustive.

4 Threats of the Internet Infrastructure

4.1 Threat types

According to the ENISA Glossary,⁹ a threat is “any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service”.

Based on the identified assets within the previous chapter a taxonomy of relevant threats impeding the Internet infrastructure or at least significant parts is developed.

Since this study focuses on information security, the threat taxonomy presented mainly covers cyber security threats. However, for faultless operation, physical assets are also required and therefore several specific non-IT threats are assumed. The identified threats are a consolidation of the publications ENISA Threat Landscape 2013,⁶ the Smart Grid Threat Landscape and Good Practice Guide,¹⁰ the Security Framework for Article 4 and 13a proposal,¹¹ and ENISA’s *Guideline on Threats and Assets*.¹² Consecutively, the first level of the threat taxonomy is presented and some instances of associated threats are provided.

The threats have been regrouped under threat types, each threat type representing the source cause of a threat. They are the following:

- **Physical attacks** are intentional offensive actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection. This threat type basically applies to any kind of infrastructure in general, thus also to the Internet infrastructure. Instances, among others, are vandalism, theft, sabotage, information leakage, and bomb attacks.
- A **disaster** is a serious disruption of the functioning of a society and can be divided into natural disasters not directly triggered by humans, and environmental disasters directly caused by human. Those threats apply to any kind of asset in general, hence also to the Internet infrastructure. Typical threats of this class are earthquakes, floods, wildfires and pollution, dust, or corrosion.
- The condition of not or insufficient functioning of any Internet infrastructure asset is defined as **failure or malfunction**. For example, failures or disruptions of network devices or systems, software bugs, or configuration errors.
- **Outages** are unexpected disruptions of service or decrease in quality falling below a required level. This includes all kinds of assets, even human resources. Outages may have many reasons, including, but not limited to, lack of resources, exhaustions, power surges, or human factors like absence of personnel.

⁹ ENISA Glossary, <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary>

¹⁰ ENISA, “Smart Grid Threat Landscape”, <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide>

¹¹ ENISA, “Security Framework for Article 4 and 13a proposal”, <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security-framework-for-articles-4-and-13a>

¹² [https://resilience.enisa.europa.eu/article-13/guideline on threats and assets/guideline-on-threats-and-assets/at_download/file](https://resilience.enisa.europa.eu/article-13/guideline%20on%20threats%20and%20assets/guideline-on-threats-and-assets/at_download/file)

- **Unintentional damage** refer to destruction, harm, or injury to property or persons by accident. Damage includes physical damage as well as information leakage, system alterations, inadequate designs, or lack of adaptation.
- **Damage** refers to destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness. The concrete threats are similar to the unintentional damage but primarily focus on IT assets and imply intention. Important representatives are such threats as loss of information, loss of reputation, and loss of hardware.
- **Nefarious activities and abuse** are intended actions that target ICT systems, infrastructure, and/or networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target. This class of the taxonomy arranges common threats generally referred to as cyber attacks and related actions such as spam, malware, hardware and software manipulation, distributed denial of service (DDoS), unauthorised usage, social engineering, or exploitation of software bugs.
- **Eavesdropping/Interception/Hijacking** refers to a class of actions aiming to listen, interrupt, or seize control of a third party communication without consent.
- **Legal** threats can be envisaged, intended, or on-going legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law. Such legal threats include violation of laws, court orders, and failure to meet contractual requirements that are carried out by or are attributed to service providers of service beneficiaries of the network infrastructure.

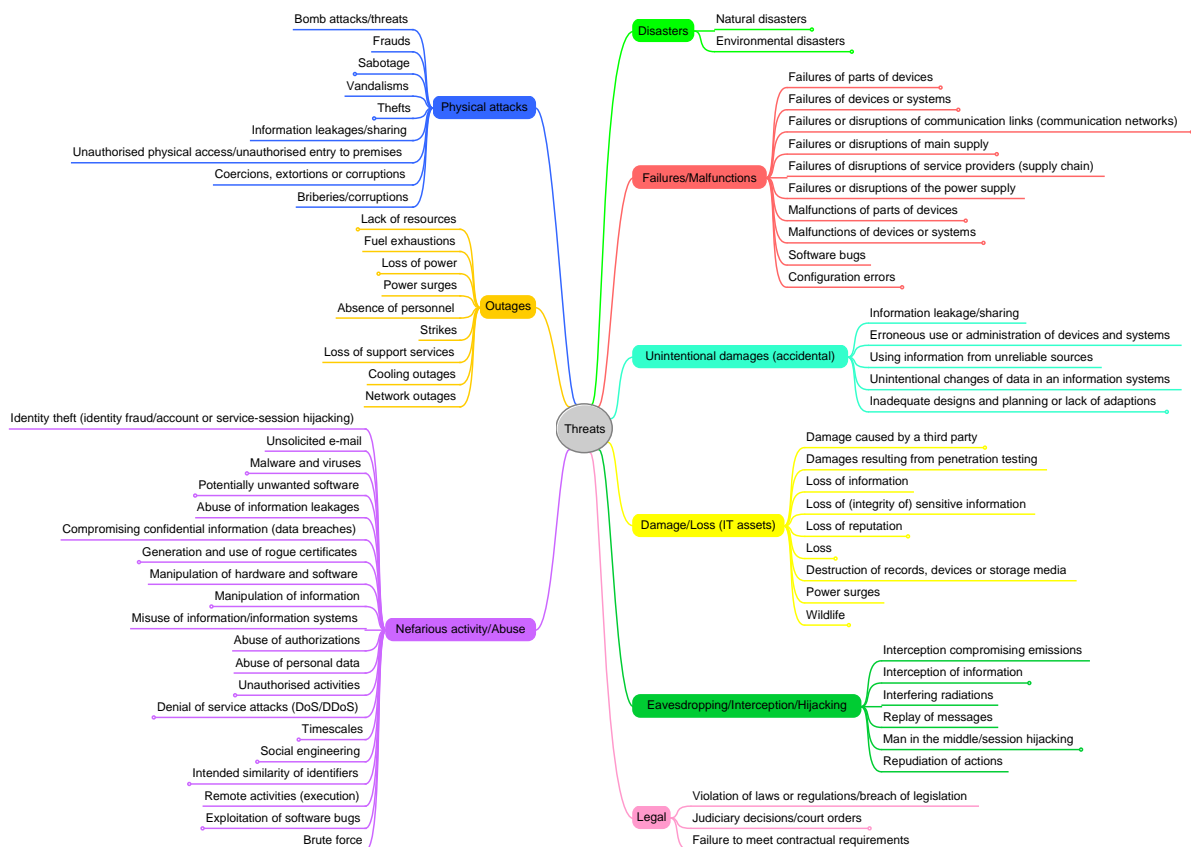


Figure 4 – Threat taxonomy of the Internet infrastructure (levels 1 and 2 - see Annex C for the expanded mind map)

The mind map presented in Figure 4 structures all identified threat types and the particular associated threats. For readability, the mind map details only the first two levels. An expanded version is presented in Annex C.



It should be noted that the details presented reflect the current state of play within the quoted reports above. However, they are subject to changes in the event of new developments and should be considered as living documents reflecting dynamic changes in the cyber threat environment.

4.2 Important Specific Threats of the Internet Infrastructure

In this chapter, threats specific to the Internet infrastructure are identified. As stated previously, the Internet is the backbone of our modern information society and thus vulnerabilities within this crucial infrastructure are not limited to single companies or some end-users, but may put a significant portion of the Internet at danger. This threatens the daily life of thousands of users. The previously developed threat taxonomy (cf. Chapter 4) includes several threats applicable to information and telecommunication technology in general, hence also to be considered for the Internet infrastructure. However, to take the scope of this study into account, the consideration of solely Internet Infrastructure threats is advisable for a deeper analysis. It admits a deeper understanding of threat details and allows concentration on the protection of relevant assets during the stock taking of the good practices in Chapter 7 below.

To identify important specific threats this study takes stock of authoritative threat reports. The material analysed has been published by private and public institutions and communities.^{13 14 15 16} For each threat the importance according to frequency of appearance, giving an estimation if no valid data could be found, and expert's judgments is evaluated. The list developed was reviewed during interviews with experts in the field and ENISA's Internet Infrastructure Security and Resilience Reference Group.¹⁷

The conclusive listing is clustered into **threat groups** according to the exposed assets. Each threat group regroups the threats menacing a particular technical domain and/or technology, with no discrimination in regard with their threat type. The main threat groups are **routing threats**, **DNS threats**, **DDoS threats**, and **generic threats** which are not specific to the Internet infrastructure as denoted above. Thus, threats and threat groups presented within this section reflect the current state-of-play but are not, and will never be exhaustive. However, one can argue that the given set of threats still have strong relevance and should be considered within risk assessments conducted by asset owners.

Subsequently, threat groups and their threats are presented. For each threat group the related threat type in the presented taxonomy is referred to, followed by a description of all subordinate specific important threats. The level of detail is limited to a certain extent to maintain readability. In order to illustrate the importance of the threat, it is supplemented with an example of a recent incident. Note that the list is not prioritised, but trends for the threat groups are provided so that asset owners can evaluate their priorities after a risk assessment.

4.2.1 Routing Threats

Routing is subject to attacks that can harm the interconnection of networks as well as the operation of single networks. A smooth operation of routing infrastructure is crucial for the robustness of the

¹³ Verizon, "2014 Data Breach Investigations Report", 2014,

http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

¹⁴ "Cloud Computing Top Threats in 2013", Cloud Security Alliance, 2013,

https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

¹⁵ "IBM Security Services Cyber Security Intelligence Index", IBM, 2013, [https://www-](https://www-935.ibm.com/services/multimedia/Cyber_security_Index.pdf)

[935.ibm.com/services/multimedia/Cyber_security_Index.pdf](https://www-935.ibm.com/services/multimedia/Cyber_security_Index.pdf)

¹⁶ "BSI Threats Catalogue", Federal Office for Information Security, 2012,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschatz/download/threats_catalogue.pdf?__blob=publicationFile

¹⁷ <https://resilience.enisa.europa.eu/internet-infrastructure-security-and-resilience-reference-group>

Internet. Most threats break down routing functions by hijacking, misusing, misconfiguring, or intercepting assigned numbers, addresses, or name spaces. The current trend indicates that this threat is on the rise.

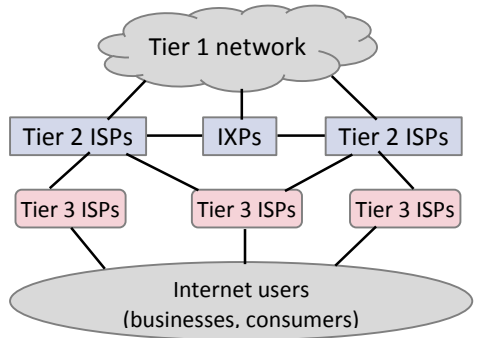
	Nefarious Activity/Abuse		Eavesdropping/Interception/Hijacking	
	Autonomous System (AS) hijacking	Address space hijacking (IP prefixes)	Route leaks	BGP session hijacking
	█	█	█	█

Table 1 – Application of Important Specific Threat to routing

Table 1 highlights the application of important specific threats to the routing infrastructure, for Tier 1 networks, Tier 2 ISPs and IXPs, Tier 3 ISPs and final users. The extent of a threat is represented by a coloured bar, which denotes how the threat applies to the layers pictured on the left-hand side schema. Routing threats apply to all layers of the Internet Infrastructure.

These important specific threats are now detailed and their trends are presented.

Threat Type: Nefarious Activity/Abuse

Trend: Increasing 

Threat: Autonomous System (AS) hijacking

AS hijacking attacks aim at impersonating a victim’s organization. The motivation behind this type of attack is malicious: activities conducted with the hijacked network are masked and appear to be carried out on the behalf of the victim itself. Such attacks are characterised by an attacker announcing the victim’s prefixes that originate at the victim’s AS.¹⁸

Example:

- A forensic case study on AS hijacking: the attacker’s perspective¹⁸

Threat: Address space hijacking (IP prefixes)

This threat occurs when a rogue BGP peer maliciously announces a victim's prefixes in an effort to reroute some or all traffic through its own networks for untoward purposes (for example, to view contents of traffic that the router would otherwise not be able to read).^{19 20 21}

Examples:

- Hacker redirects traffic from 19 Internet providers to steal bitcoins²²
- Hijack by AS4761 – Indosat, a quick report²³

¹⁸ “A Forensic Case Study on AS Hijacking: The Attacker’s Perspective”, <http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf>

¹⁹ “Protecting Border Gateway Protocol for the Enterprise”, http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html

²⁰ “Beware of BGP Attacks”, <http://www.cc.gatech.edu/~dovrolis/Papers/ccr-bgp.pdf>

²¹ “Threat Model for BGP Path Security”, <http://tools.ietf.org/html/rfc7132>

²² <http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit>

- The new threat: targeted Internet traffic misdirection²⁴
- Looking at the Spamhaus DDoS from a BGP perspective²⁵
- Pakistan hijacks YouTube²⁶

Threat Type: Eavesdropping/Interception/HijackingTrend: Increasing ⁶**Threat: Route leaks**

A route leak is said to occur when AS A advertises BGP routes that it has received from AS B to its neighbors, but AS A is not viewed as a transit provider for the announced prefixes.²⁷

Examples:

- Hijack by AS4761 – Indosat, a quick report²³
- How the Internet in Australia went down under²⁸
- Large route leaks²⁹

Threat: BGP session hijacking

BGP session hijacking denotes an alteration of the contents of the BGP routing table by a malicious device, which can, among other impacts, prevent traffic from reaching the intended destination without acknowledgement or notification.^{30 31 32}

Example:

- Short-Lived BGP Session Hijacking³³
- *Measuring and Analyzing on Effectation of BGP Session Hijack Attack*³⁴

4.2.2 DNS Threats

The **DNS** system is exposed to threats that aim to bring down a central feature which allows convenient web browsing for non-technical users and enables flexible addressing for automated systems. Without the resolution of domain names into IP addresses the Internet is inaccessible for the general public. Attacks attempt to alter DNS records to redirect traffic, interrupt operation, or introduce censorship. The latest trends show a decrease for this sort of threat. However, this does not diminish its importance.

²³ <http://www.bgpmn.net/hijack-by-as4761-indosat-a-quick-report>

²⁴ <http://www.renesys.com/2013/11/mitm-internet-hijacking/>

²⁵ <http://www.bgpmn.net/looking-at-the-spamhouse-ddos-from-a-bgp-perspective/>

²⁶ <http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/>

²⁷ "Threat Model for BGP Path Security", <http://tools.ietf.org/html/rfc7132>

²⁸ <http://www.bgpmn.net/how-the-internet-in-australia-went-down-under/>

²⁹ <http://nrl.cs.arizona.edu/projects/lslr-events-from-2003-to-2009/>

³⁰ "Protecting Border Gateway Protocol for the Enterprise", http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html

³¹ "Beware of BGP Attacks", <http://www.cc.gatech.edu/~dovrolis/Papers/ccr-bgp.pdf>

³² "Threat Model for BGP Path Security": <http://tools.ietf.org/html/rfc7132>

³³ <https://www.usenix.org/publications/login/december-2006-volume-31-number-6/homeless-vikings-short-lived-bgp-session-hijack/>

³⁴ "Measuring and Analyzing on Effectation of BGP Session Hijack Attack", <http://www.wseas.us/e-library/conferences/2013/Rhodes/CIRCOM/CIRCOM-13.pdf>

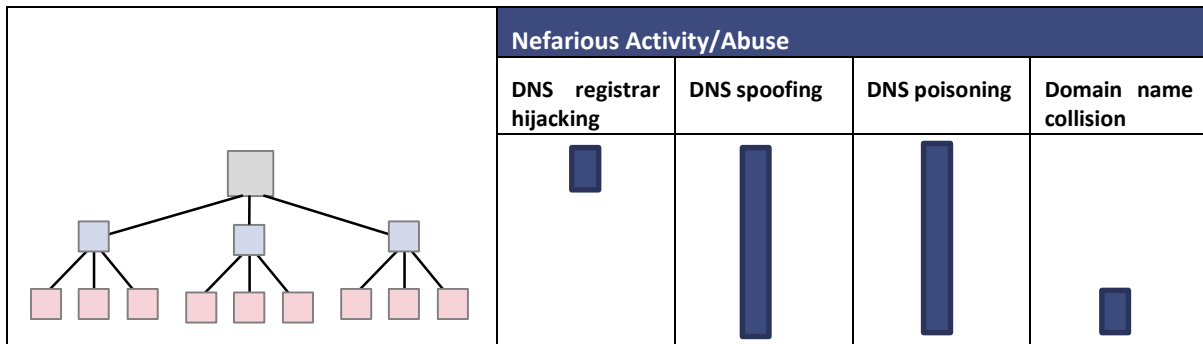


Table 2 – Application of Important Specific Threat to DNS

Table 2 highlights the application of important specific threats to the DNS infrastructure. The DNS infrastructure is represented by an abstract (simplified) tree, which shows a combination of several typical layers. The extent of a threat is represented by a coloured bar, which denotes how the threat applies to the layers pictured on the left-hand side schema. Important specific threats for DNS apply to different extents to the Internet Infrastructure.

These important specific threats are now detailed and their trends are presented.

Threat Type: Nefarious Activity/Abuse

Trend: Decreasing 

Threat: DNS registrar hijacking

If a DNS registrar is hijacked, all domains under its control are in jeopardy: the domain registration information can be altered, which might result in a transfer of the domain to another registrar or result in a type of identity theft. Once this has been done, the hijacker has full control of all the domains and can use them or sell them to a third party.³⁵

Example:

- Popular registrar Namecheap fixes DNS hijack bug³⁶

Threat: DNS spoofing

DNS spoofing refers to the broad category of attacks that spoof DNS records. There are many different ways to do DNS spoofing: compromise a DNS server, mount a DNS cache poisoning attack, mount a man-in-the-middle attack, guess a sequence number, and many more.

Example:

- Subverting BIND’s SRTT algorithm derandomizing NS selection³⁷

Threat: DNS poisoning

DNS (cache) poisoning is an attack technique that allows an attacker to introduce forged DNS information into the cache of a caching domain name server. There are published articles that describe a number of inherent deficiencies in the DNS protocol and defects in common DNS implementations that facilitate DNS cache poisoning.³⁸

Examples:

- Abusing anti-DDoS mechanisms to perform DNS cache poisoning³⁹
- Fragmentation considered poisonous⁴⁰

³⁵ “Popular Registrar Namecheap Fixes DNS Hijack Bug”, <http://threatpost.com/popular-registrar-namecheap-fixes-dns-hijack-bug>

³⁶ <http://threatpost.com/popular-registrar-namecheap-fixes-dns-hijack-bug>

³⁷ <https://www.usenix.org/conference/woot13/workshop-program/presentation/hay>

³⁸ “Multiple DNS implementations vulnerable to cache poisoning”, <http://www.kb.cert.org/vuls/id/800113>

³⁹ <http://www.ssi.gouv.fr/en/the-anssi/publications-109/scientific-publications/conference/abusing-anti-ddos-mechanisms-to-perform-dns-cache-poisoning.html>

Threat: Domain name collision

A name collision refers to an attempt to resolve a name that is utilised in a private name space (e.g. non-delegated Top Level Domain, or a short, unqualified name), resulting in a DNS query to the public DNS, and a matching name can be retrieved. In most cases, the cause is a misconfiguration and disregards ICANN recommendations. Name collision occurrences are not new and have historically been observed and reported as queries containing non-delegated TLDs at the root level of the DNS. They have received renewed attention because many applied for new TLD strings that are identical to name space labels used in private networks.⁴¹

Examples:

- Looking at corp.com as a proxy for .corp⁴²
- Reports for alternate path to delegation published⁴³

4.2.3 Denial of Service (DoS/Distributed DoS (DDoS)) Threats

Denial of service attacks endeavour to make a computer system or network unavailable to its intended users. Basically, every single system can be targeted by DoS ranging from a simple home computer to a major web server farm. There are several different approaches which amplify the intensity of an attack. Especially this kind of attack is increasing these days.

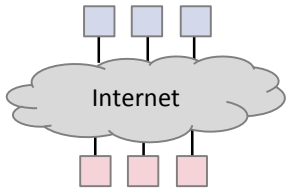
	Nefarious Activity/Abuse				
	DDoS amplification /reflection	DoS flooding	DoS protocol exploitation	DoS malformed packet attack	DoS application attack
	■	■	■	■	■

Table 3 – Application of Important Specific Threat to Denial of Service

Table 3 highlights the application of important specific threats regarding Denial of Service. The Internet architecture shown in the picture is simplified and abstracted in order to show the important parts in regard to DoS. The extent of a threat is represented by a coloured bar, which denotes how the threat applies to the layers pictured on the left-hand side schema. Important specific threats for DoS apply to different extents to the Internet Infrastructure.

These important specific threats are now detailed and their trends are presented.

Threat Type: Nefarious Activity/Abuse

Trend: Increasing ⁶

Threat: DDoS amplification/reflection

In a reflection DDoS attack, the attacker spoofs the victim’s IP address and sends a request for information via UDP to servers known to respond to that type of request. The servers answer the request and send the response to the victim’s IP address. All data from those servers adds up to

⁴⁰ <http://arxiv.org/abs/1205.4011>

⁴¹ “Name Collision in the DNS”, <https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf>

⁴² http://namecollisions.net/downloads/wpnc14_slides_strutt_looking_at_corpcom.pdf

⁴³ <http://newgtlds.icann.org/en/announcements-and-media/announcement-2-17nov13-en>

significant bandwidth, enough to congest the target's Internet connectivity. With bandwidth maxed out, normal traffic cannot be serviced and legitimate clients cannot connect.⁴⁴

Examples:

- The technical details behind a 400 Gbps NTP amplification DDoS attack⁴⁵
- Deep inside a DNS amplification DDoS attack⁴⁶
- The DDoS that knocked Spamhaus offline (and how we mitigated it)⁴⁷

Threat: DoS flooding

A flood is a simple denial-of-service attack where the attacker overwhelms the victim with packets (e.g. ICMP ping packets). It is most successful if the attacker has more bandwidth than the victim (for instance, an attacker with a DSL line and the victim on a dial-up modem). The attacker may hope that the victim will respond to its packets (e.g. ICMP echo reply packets), thus consuming both outgoing bandwidth as well as incoming bandwidth.

Examples:

- Low Orbit Ion Cannon⁴⁸
- Anonymous Declares Cyber War on Israel, Downs Mossad Site, Many Others⁴⁹

Threat: DoS protocol exploitation

Protocol exploitation (e.g. TCP-SYN) is a form of denial-of-service attack in which an attacker sends a succession of requests to a target's system in an attempt to consume enough server resources (e.g. TCP ports) to make the system unresponsive to legitimate traffic.

Examples:

- DDoS attacks exploiting vulnerability in network time protocol, call the doctor⁵⁰
- Slowloris DoS attack, aka "Slow and low"⁵¹

Threat: DoS malformed packet attack

Attacks designed to crash an operation system's network stack by providing malformed header information or payload.⁵²

Examples:

- Massive 300 Gbps DDoS Attack on Media Firm Fuelled by Unpatched Server Flaw⁵³
- Vulnerability in ICMPv6 could allow Denial of Service⁵⁴

Threat: DoS application attack

Known application logic limitations, flaws and vulnerabilities are exploited, resulting in a specific application failure or data corruption.

Examples:

⁴⁴ "Reflection DDoS Attacks: How They Work and What You Can Do",

<http://www.ddosattacks.biz/attacks/reflection-ddos-attacks-how-they-work-and-what-you-can-do/>

⁴⁵ <http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack>

⁴⁶ <http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack>

⁴⁷ <http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho>

⁴⁸ http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

⁴⁹ <http://blackbag.gawker.com/anonymous-declares-cyber-war-on-israel-downs-mossad-si-1615500861>

⁵⁰ <http://www.itcsecure.com/2014/01/ddos-attacks-exploiting-vulnerability-in-network-time-protocol-call-the-doctor/>

⁵¹ <http://www.ddosattacks.biz/attacks/slowloris-ddos-attack-aka-slow-and-low/>

⁵² <http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf>

⁵³ <http://www.computerworld.in/news/massive-300gbps-ddos-attack-on-media-firm-fuelled-by-unpatched-server-flaw>

⁵⁴ <https://technet.microsoft.com/library/security/ms13-065>

- Gartner says 25 percent of distributed denial of services attacks in 2013 will be application-based⁵⁵
- DDoS attack used 'headless' browsers in 150-hour siege⁵⁶

4.2.4 Generic Threats

All threats mentioned in the generic threats category apply to all computer systems in general, hence also to systems of the Internet infrastructure. It is a summary of important threats rather than a complete list and should raise awareness that even very common attacks may harm the Internet infrastructure.

Threat Type: Physical attack

Trend: Not available

A physical attack can constitute a threat to an organization, certain areas of the organization or individuals. The technical possibilities to perpetrate an attack are numerous: throwing bricks, blasts by explosives, use of firearms or arson.⁵⁷

Threat Type: Damage/Loss

Trend: Increasing 

Any incident where a) an asset (e.g. sea-cable, device, information) is damaged by accident or in bad faith or b) an asset (e.g. storage media, documents) goes missing, whether through misplacement or malice.¹³

Threat Type: Failures/Malfunctions

Trend: Increasing 

Threat: Failure of devices or systems

Due to dependencies of technical infrastructure, single failures of individual components, such as air-conditioning or power supply facilities, may contribute to the failure of a device or even the entire system. In particular, key components of an IT system (for example, servers and network coupling elements) are likely to cause such failures.⁵⁹

Threat: Configuration errors

Configuration error attacks exploit configuration weaknesses found in software. Software may come with unnecessary and unsafe features, such as debug and QA features, enabled by default. These features may provide a means for an attacker to bypass authentication methods and gain access to sensitive information, perhaps with elevated privileges. Likewise, default installations may include well-known usernames and passwords, hard-coded backdoor accounts, special access mechanisms, and incorrect permissions set for files accessible through web servers. Default samples may be accessible in production environments. Configuration files that are not properly locked down may reveal clear text connection strings to the database, and default settings in configuration files may not have been set with security in mind. All of these misconfigurations may lead to unauthorised access to sensitive information.⁶⁰

⁵⁵ <http://www.gartner.com/newsroom/id/2344217>

⁵⁶ <http://www.darkreading.com/attacks-breaches/ddos-attack-used-headless-browsers-in-150-hour-siege/d/d-id/1140696?>

⁵⁷ "Threats Catalogue – Elementary Threats",

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf

⁵⁸ "ENISA Annual Incident Reports 2013", http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport

⁵⁹ "Threats Catalogue – Elementary Threats",

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?_blob=publicationFile

⁶⁰ "Application Misconfiguration",

<http://projects.webappsec.org/w/page/13246914/Application%20Misconfiguration>

Threat Type: Nefarious activity/AbuseTrend: Increasing ⁶**Threat: Malware and viruses**

Malware, short for malicious software, is a generic term for any program with the intention of disrupting computer operation, gathering sensitive information or gaining access to private computer systems. It encompasses, among others, viruses, worms, trojans, rootkits, botnets, spyware, scareware, or rogueware.^{61 62}

Threat: Brute force

Brute force attacks are often used to defeat a cryptographic scheme, such as those secured by passwords. Hackers use computer programs to try a very large number of passwords to decrypt the message or access the system.⁶³

Threat: Social engineering

Social engineering is the psychological manipulation of human behavior to breach security without the participants (or victims) even realizing they have been manipulated. There are two main categories under which all social engineering attempts could be classified – computer- or technology-based deception, and human-based deception. The technology-based approach is to deceive the user into believing he is interacting with the ‘real’ computer system and get him to provide confidential information. The human approach is done through deception, by taking advantage of the victim’s ignorance and the natural human inclination to be helpful and liked.⁶⁴

Threat: Data breach

A data breach refers to the exfiltration of data from a system without the knowledge or consent of its owner. This data resides in the targeted organization’s systems or networks and is proprietary or sensitive in nature. Propriety data may be valuable or confidential in nature to an organization. Acquisition by external parties may cause harm. This data can comprise personally identifiable information, customer data, trade secrets and the like.⁶⁵

Threat Type: Eavesdropping/Interception/HijackingTrend: Increasing ⁶⁶**Threat: Espionage**

Espionage is a process that involves human sources or technical means to obtain information that normally is not publicly available.⁶⁷

4.3 Summary of threat trends

This section sums up the trends for each threat type presented in the previous section. The general tendency denotes an increase for the majority of threats, as presented in Table 4.

⁶¹ Y. ROBIAH et al., “A new generic taxonomy on hybrid malware detection technique”, arXiv preprint, <http://arxiv.org/abs/0909.4860>

⁶² Joanna RUTKOWSKA, “Introducing stealth malware taxonomy”, COSEINC Advanced Malware Labs, 2006, S. 1-9

⁶³ “Brute force attack”, <http://www.sophos.com/en-us/threat-center/threat-analyses/threatsaurus/a-to-z-of-threats/b/brute-force-attack.aspx>

⁶⁴ “The Threat of Social Engineering and Your Defense Against It”, <http://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232>

⁶⁵ “Anatomy of a Data Breach”, <http://about-threats.trendmicro.com/us/webattack/110/Anatomy-of+a+Data+Breach>

⁶⁶ Hackmageddon Analysis, <http://hackmageddon.com/2013-cyber-attacks-statistics/>

⁶⁷ “What is Espionage”, <https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html>

However, this result shall be mitigated for some Important Specific Threat by the actual number of attacks using this threat. An increasing trend denotes a greater number of occurrence this year compared to the previous year, even though the number of attacks can be low. An increasing trend for this can of threats should be an incentive to monitor potential attacks in the future.

On another hand, a decreasing trend for Important Specific Threat does not diminish the importance of this threat. In the table, DNS Threat is decreasing. Yet, the number of cyber attacks targeting DNS remains important in relation to the total number of attacks. This decreasing trend shall only denote a diminution of DNS as an attack vector by threat agents.









Threat groups	Threat types	Trends
Routing Threats	Nefarious Activity/Abuse	Increasing 
	Eavesdropping/Interception/Hijacking	Increasing 
DNS Threats	Nefarious Activity/Abuse	Decreasing 
Denial of Service	Nefarious Activity/Abuse	Increasing 
Generic Threats	Physical attack	N/A
	Damage/Loss	Increasing 
	Failures/Malfunctions	Increasing 
	Nefarious activity/Abuse	Increasing 
	Eavesdropping/Interception/Hijacking	Increasing 

Table 4 – Summary of trends per threat type for each threat group

5 Internet Infrastructure Assets Exposure to Cyber Threats

In this section the threat exposure of Internet infrastructure is presented. The association between the assets from Figure 3 and the threats from Figure 4 is established for every threat type. An interested reader can identify relevant threats based on its deployed assets. Table 5 matches a selection of given threats with the assets types involved. Annex D proposes a more exhaustive list of threats and their relevant assets.

The information depicted within the table are arranged as follows:

- **Threat types:** This column states the threat types.
- **Threats:** This field contains more detailed threats which belong to the different threat types.
- **Asset types:** This field specifies by the threats and threat types exposed asset types.

Threat types	Threats	Asset types
Physical attacks		
	Sabotage	Hardware, Infrastructure
	Unauthorised physical access/unauthorised entries to premises	Hardware, Infrastructure
Disasters		
	Natural disasters	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Environmental disasters	<i>Ditto</i>
Failures/Malfunctions		
	Failures of parts of devices	Protocols, Hardware, Software, Information, Services
	Configuration errors	Protocols, Hardware, Software, Information, Services
Outages		
	Lack of resources	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Network outages	Hardware, Software, Information, Services
Unintentional damages (accidental)		
	Information leakage/sharing	Hardware, Software, Information, Services, Interconnection
	Unintentional change of data in an information systems	Protocols, Hardware, Software, Information, Services
Damage/Loss (IT assets)		
	Damage caused by a third parties	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Loss of reputation	Interconnection, Human resources

Threat types	Threats	Asset types
Nefarious activity/Abuse		
	Manipulation of hardware and software	Protocols, Hardware, Software, Information, Services
	Denial of service attacks (DoS/DDoS)	Hardware, Software, Information, Services
Eavesdropping /Interception/Hijacking		
	Interception compromising emissions	Protocols, Software, Information, Services
	Man in the middle/session hijacking	Software, Information, Services
Legal		
	Violations of law or regulation/breaches of legislation	Software, Information, Interconnection, Human resources
	Failure to meet contractual requirements	<i>Ditto</i>

Table 5 – Association between threats and assets (excerpt. See Annex D for the exhaustive list)

6 Threat Agents

According to ENISA Threat Landscape 2013,⁶ a threat agent is “someone or something with decent capabilities, a clear intention to manifest a threat and a record of past activities in this regard”. Once again, this study only yields a generic overview because of the lack of a concrete implementation. For Internet infrastructure asset owners, it is crucial to be aware of which threats emerge from which threat agent group. Table 6 presents such an overview.

However, this study does not develop a new glossary on threat agents within the IITL, but rather utilises the ENISA Threat Landscape 2013’s consolidation of several publications.^{68 69 70 71 72 73 74} Interested readers may find a detailed description in ENISA’s Threat Landscape 2013.⁶ The classification of threat agents is as follows:

- Corporations
- Hacktivists
- Cyber criminals
- Cyber terrorists
- Script kiddies
- Online social hackers
- Employees
- Nation states

Based on the threat agents the threats are assigned to relevant threat types (cf. Table 6). A detailed overview covering not only the threat types is given in Annex E.

	Corporations	Hacktivists	Cyber criminals	Cyber terrorists	Script kiddies	Online social hackers	Employees	Nations states
Physical attacks	✓	-	✓	✓	-	-	✓	✓
Disasters	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Failures/ Malfunctions	✓	-	-	-	-	-	✓	-
Outages	✓	✓	✓	✓	✓	✓	✓	✓
Unintentional damages	✓	-	-	-	-	-	✓	-
Damage/Loss	✓	✓	✓	✓	✓	✓	✓	✓
Nefarious activity/Abuse	✓	✓	✓	✓	✓	✓	✓	✓
Eavesdropping/ Interception/ Hijacking	✓	✓	✓	✓	✓	✓	✓	✓
Legal	✓	✓	✓	✓	✓	✓	✓	✓

Table 6 – Involvement of threat agents in threats

⁶⁸ <https://www.ncsc.nl/english/current-topics/news/cyber-security-assesment-netherlands.html>

⁶⁹ <http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf>

⁷⁰ http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=302:hackers-profiling-who-are-the-attackers&catid=50:issue-7&Itemid=187

⁷¹ <http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background>

⁷² <http://www.verizonenterprise.com/DBIR/2013/>

⁷³ <http://owasptop10.googlecode.com/files/OWASP%20Top%20%20%20%202013.pdf>

⁷⁴ <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/global-profiles-of-the-fraudster/Documents/global-profiles-of-the-fraudster-v2.pdf>

7 Good Practices

This section takes stock of publicly available security measures to protect Internet infrastructure assets and thereby supports the resilience of the Internet ecosystem. Therefore, different sources with recommendations and good practices published by major Internet institutions or working groups such as ICANN, IETF, RIPE, Euro-IX, and Internet Society are reviewed, summarised, and mapped to the previously identified important specific threats. This tool enables asset owners to carefully analyse their infrastructure and adopt appropriate good practices. The entire list including all references can be found in Annex F.

A central design principle of the Internet, as a collection of networks, is shared responsibility. Every participant should be conscious that their own security also depends on the security of neighbouring networks. Hence, it is a collective responsibility to implement good practices when deemed useful for their own security, and for the security of other parties when applicable. An example is insufficiently configured DNS or NTP servers that are used by adversaries to amplify DDoS attacks.

One must be aware of the fact that the given list is not exhaustive. However, in order to ensure a certain level of quality, the list has been reviewed by acknowledged experts in the field and the ENISA Internet Infrastructure Security and Resilience Reference Group.⁸

Table 7 contains the identified good practices and gives more details regarding the gap analysis. It does not present good practices for “Generic Threats” which are, as their name implies, too generic to be addressed by specific good practices. The table is structured as follows:

- **Important specific threat groups:** A line with a grey background which contains the important specific threat groups defined in section 4.2.
- **Threats:** Here are the concrete threats, grouped according to the previous column, which denote the actual threats which should be countered by applying the good practices.
- **Good practices:** The actual good practices for the threat in the same row. The description is a summary of different sources which are referenced in Annex F.
- **Assets, assets covered:** All assets related to an important specific threat group are printed in black. In the rows of the concrete threats, all assets covered by at least one measure are printed in green.
- **Gap (assets not covered):** This column contains the assets related to a threat which are not covered by the associated good practice, printed in black. If an asset is not covered by at least one good practice within the distinct threat group, this asset is printed in red to highlight it as a gap for the threat type.



Threats	Good practices	Assets, <i>assets covered</i>	<i>Gaps</i> (assets not covered)
Routing threats			
AS hijacking		Internet protocol addressing, Routing protocols, Administrators	Administrators
	Utilise resource certification (RPKI) to provide AS origin validation. Reader must be aware that at the time of writing, it is no possible to detect AS hijacking automatically.	Internet protocol addressing, Routing protocols	Administrators
Address space hijacking (IP prefixes)		Routing, Internet protocol addressing, System configurations, Network topology	-
	Utilise resource certification (RPKI) to provide AS origin validation.	Routing, Internet protocol addressing, System configurations, Network topology	
	Establish an Appropriate Use Policy (AUP) as explained in BCP 46, which promotes rules to secure peering.	Routing, Internet protocol addressing, System configurations, Network topology	
	Establish ingress filtering from the edge site to the Internet.	Routing, Internet protocol addressing	System configurations, Network topology
	Establish Unicast Reverse Path Forwarding to verify the validity of a source IP address.	Routing, System configurations, Network topology	Internet protocol addressing
	Establish egress filtering at the boundary router to proactively filter all traffic going to the customer that has a source address of any of the addresses that have been assigned to that customer.	Routing, Internet protocol addressing	System configurations, Network topology
	Filter the routing announcements and implement techniques that reduce the risk of putting excessive load on routing generated by illegitimated route updates/announcements. For instance, Route Flap Damping (RFD) with a well-defined threshold may contribute to reducing router processing time.	Routing, Network topology	Internet protocol addressing, System configurations
	Registry databases such as IRR, APNIC, ARIN, and RIPE have to be subject to continuous maintenance. This shall allow usage of updated information to secure peering. For example, the "Route Object" field can help validating routes received from peers.	Routing, Internet protocol addressing, System configurations	Network topology
	Configuration updates for the routing infrastructure may only be performed by a defined authority using strong authentication.	Routing, System configurations, Network topology	Internet protocol addressing
Route leaks	Monitor the status of BGP to detect unusual behaviour such as path changes or unusual announcement.	Routing, Internet protocol addressing, System configurations, Network topology	
		Routing, Network topology	-
	Configure BGP <i>maximum-prefix</i> to ensure the validity of routes announced. If more prefixes are received, it is sign of an incorrect behaviour and the BGP session shuts down.	Routing, Network topology	
BGP session hijacking	Utilise resource certification (RPKI) to provide AS origin validation.	Routing, Network topology	
		Routing, Internet protocol addressing, System configurations, Network topology	-
	Establish prefix filtering and automation of prefix filters.	Routing, Internet protocol addressing, System configurations, Network topology	
	Employ AS path filtering.	Routing, Internet protocol addressing, System configurations, Network topology	
	Use TCP-AO (TCP-Authentication Option) to secure BGP Authentication in order to replace TCP-MD5. TCP-AO simplifies the exchange of keys.	Routing, Internet protocol addressing, System configurations, Network topology	

Threats	Good practices	Assets, assets covered	Gap (assets not covered)
DNS Threats			
DNS registrar hijacking		Domain name system, Addressing units, Applications, Credentials, Administrators	-
	Registrants must protect account credentials and define authorised users, while registrars have to provide a secure authentication process.	Addressing units, Credentials, Administrators	Domain name system, Applications
	Registrants should take advantage of routine correspondence from registrar such as change notification, billing information, or WHOIS records. Hence, registrars must provide such information.	Addressing units, Applications	Domain name system, Credentials, Administrators
	Registrants should maintain documentation to “prove registration”.	Addressing units, Applications	Domain name system, Credentials, Administrators
	Registrants should use separate identities for registrant, technical, administrative, and billing contacts. Thus, registrars need to allow a more complex user rights management.	Credentials, Administrators	Domain name system, Addressing units, Applications
	Registrars must establish an effective zone data management.	Domain name system, Addressing units, Applications	Credentials, Administrators
	Registrars should consider supporting DNSSEC.	Domain name system, Addressing units, Applications	Credentials, Administrators
	Registrars may monitor DNS change activities.	Addressing units, Applications, Administrators	Domain name system, Credentials
DNS spoofing		Domain name system, Addressing units, Applications, System configurations, Essential addressing protocols – DNS, Administrators	Administrators
	Deploying DNSSEC aims to secure DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity.	Domain name system, addressing units, Applications, System Configurations, Essential addressing protocols – DNS	Administrators
DNS poisoning		Domain name system, Addressing units, Applications, System configurations, Executable programs, Essential addressing protocols – DNS, Administrators, Operators	Administrators, Operators
	Deploying DNSSEC aims to secure DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity.	Domain name system, Addressing units, Applications, System configurations, Executable programs, Essential addressing protocols – DNS	Administrators, Operators
	Restrict zone transfers to reduce load on systems and network.	Applications, Executable programs	Domain name system, Addressing units, System configurations, Essential addressing protocols – DNS, Administrators, Operators
	Restrict dynamic updates to only authorised sources in order to avoid misuse. Such misuse include the abuse of a DNS server as an amplifier, DNS cache poisoning...	Addressing units, applications, System configurations, Executable programs	Domain name system, Essential addressing protocols – DNS, Administrators, Operators
	Set up the authoritative name server as non-recursive. Separate recursive name servers from the authoritative name server.	Domain name system, Addressing units, Applications, Executable programs	System configurations, Essential addressing protocols – DNS, Administrators, Operators
	Allow DNS transport over TCP to support non-standard queries. Moreover, TCP may be necessary for DNSSEC.	Addressing units, Applications, System configurations, Executable programs	Domain name system, Essential addressing protocols – DNS, Administrators, Operators

Threats	Good practices	Assets, assets covered	Gap (assets not covered)
Domain name collision		Domain name system, Applications	-
	Do not use random domain names that you do not own for your internal infrastructure. For example, do not consider private domain name space as top-level domains.	Domain name system, Applications	
	Preventing DNS request for internal namespaces to leak into the Internet by applying firewall policies.	Applications	Domain name system
	Use reserved TLDs such as .test, .example, .invalid, or .localhost.	Domain name system, Applications	
Denial of Service			
Amplification / reflection		Applications, security, Generic Internet provider, Hardware, Executable programs, System configuration, Application protocols, Administrators, Operators	System configuration, Essential addressing protocols, Administrators, Operators
	Adopt source IP address verification at the edge of Internet infrastructure (close to the origin of traffic) to prevent network address spoofing through ingress and egress filtering.	Applications, Security, Generic Internet provider, Hardware, Executable programs, Application protocols	System configuration, Administrators, Operators
	Operators of authoritative name server operator should implement RRL (Response Rate Limiting).	Applications, Security, Generic Internet provider, Hardware, Executable programs	System configuration, Application protocols, Administrators, Operators
	DNS name server operators and ISPs need to disable open recursion on name servers and may only accept DNS queries from trusted sources.	Applications, Security, Generic Internet provider, Hardware, Executable programs	System configuration, Application protocols, Administrators, Operators
Flooding		Applications, Security, Generic Internet providers, Hardware, Executable programs, System configuration, Essential addressing protocols, Administrators, Operators	System configuration, Essential addressing protocols, Administrators, Operators
	Manufacturers and configurators of network equipment should take steps to secure all devices. One possibility is to keep them up-to-date by patching flaws.	Applications, Security, Generic Internet providers, Hardware, Executable programs	System configuration, Essential addressing protocols, Administrators, Operators
Protocol exploitation	-	Applications, Security, Generic Internet providers, Hardware, Executable programs, System configuration, Essential addressing protocols, Administrators, Operators	-
Malformed packet attack	-	Applications, Security, Generic Internet providers, Hardware, Executable programs, System configuration, Essential addressing protocols, Administrators, Operators	-
Application	-	Applications, Security, Generic Internet provider, Hardware, Executable programs, System configuration, Application protocols, Administrators, Operators	-

Table 7 – Threats with good practices for mitigation and the coverage of assets

7.1 Gap Analysis

Accordingly, the assets covered by at least one good practice are compared to the complete list of all assets (cf. Chapter 3) endangered by a specific important threat. This gap analysis clearly outlines existing shortcomings of this study, which are tackled by recommendations (cf. Chapter 8).

The summarised results of the gap analysis presented in Table 7 are that for most important specific threats publicly available good practices are on hand. The gaps found for every threat group are as follows:

Routing Threats

- **AS hijacking**

Gap found: Administrators

Administrators are human resources responsible to define routing rules and security levels. For instance, they define the filters applicable to BGP announcements and monitor the status of BGP. Administrators of an Internet infrastructure are usually in direct relationship with administrators of other (peer) networks and cooperate closely with them.

Available good practices for routing cover technical aspects related to filtering and monitoring. However, no good practice exists today that prevents an administrator to define rules that impact routing in a bad way, either at local or a more global scale.

Moreover, administrators ensure the security of routing by monitoring the status of their routing system used (e.g., BGP) and defining actions to take in case of an incident. However, there is currently no good practice available that clearly focuses on how to handle routing incidents between different networks. Indeed, such incidents are often resolved by contacting other administrators on an ad-hoc basis.

This gap calls for the development of good practices that shall enhance the collaboration between administrators, with the objective to secure routing and handle incidents.

DNS Threats

- **DNS Spoofing**

Gap found: Administrators

Similarly to routing, administrators are responsible for DNS security. However, spoofing can be performed when administrators fail at securing certain vulnerable assets (e.g., configure a DNS server in a secure way) in their infrastructure. For that purpose, administrators may need to perform an overview of their current security level and evaluate the assets to cover with good practices.

As previously, there is a need of collaboration in the community especially as DNS is distributed system with many different organisations involved. Indeed, spoofing can be mitigated when administrators of Internet infrastructure exchange with their peers to prevent, detect and overcome incidents.

- **DNS Poisoning**

Gap found: Administrators

This gap is identical to the one found for administrator in the threat “DNS Spoofing”. The conclusions are identical.

Gap found: Operators

Operators of DNS infrastructures are responsible to develop security rules that administrators can apply to Internet infrastructure assets. However, humans are not immune to mistakes. Moreover, the effect of certain technical security rule may differ depending on the specificities of a given Internet infrastructure.

This gap can be mitigated by evaluating the application of good practices in the protection of the Internet infrastructure. Operators can also report on the application of good practices to their particular infrastructure, in order to benefit the community.

- **Denial of Service / Flooding**

Gap found: System configuration

System configuration should ensure the application of a security policy. However, depending on the values of certain parameters and the specificities of the Internet Infrastructure, it may lead to different outcomes.

No good practice exists today to ensure protection against Denial of Service / Flooding by defining a system configuration for a given Internet infrastructure asset.

In order to validate the good usage of system configuration and improve security, the community can share experience on the configuration used to secure their Internet infrastructure, by focusing on specific use cases.

Gap found: Essential addressing protocols

In the majority of Denial of Service / Flooding cases, essential addressing protocols are spoofed when the protocol permits it (e.g., IP source addresses in UDP packets). Also, if essential addressing protocols are not spoofed the difference from flooding and a high rate of regular requests are difficult to tell for machines as it requires an understanding of purpose. In that regard, no existing good practice exist to prevent this structural issue.

This gap can be covered by evaluating specific security measures to protect connected devices. Moreover, migration toward more secured protocols can mitigate this threat to a certain extent.

Gap found: Administrators

This gap is identical to the one found for the threat groups "Routing" and "DNS". The conclusions are identical.

Gap found: Operators

This gap is identical to the gap found for the threat groups "Routing" and "DNS". The conclusions are identical.

For every threat group, the human resources asset types are inadequately covered. This is probably due to the technical focus of the reviewed material. Hence, it is advisable for asset owners to consider the human factor, besides the technical good practices, in their security strategy.

Additionally, the good practices do not cover the threat flooding for the assets *System configuration* and, *Application protocols*. This results from a more structural issue. Flooding exploits sheer data volume to disrupt a system or service, hence misconfiguration or outdated protocols are not necessarily a precondition. Thus, the considered good practices do not describe counter measures.

8 Recommendations

Based on the insights gained within this study recommendations for understanding and improving the security of the Internet infrastructure are listed in this section. Therefore, the stock taken assets and threats are condensed to important specific threat groups of the Internet Infrastructure. On this foundation and additional input of experts on good practices have been collected and summarised.

The following gap analysis yields a number of assets that cannot be covered by at least one good practice. In order to provide information for the protection of not adequately covered assets, a set of recommendations has been developed. Finally, the recommendations were reviewed by ENISA experts and the reference group for Internet Infrastructure Security and Resilience.¹⁷

The list of recommendations is divided into technical (Section 8.1) and organisational (Section 8.2) guidance to address particular target audiences. They may be considered by relevant stakeholders such as standardization bodies (e.g., IETF, ICANN), industry, and academia.

One must be aware of the fact that no list of good practices and recommendations can be exhaustive nor is it feasible to maintain a list of all possible protection measures. It is important to raise the bar high enough to provide a baseline security at the very least.

The scope of this study is the Internet infrastructure; this study strongly advocates depending on the core business of a company, the implementation and tailoring of the good practices for routing, DNS, and DDoS mitigation listed in Chapter 7. Additionally, it should be kept in mind that hardware vendors for core Internet devices such as routers or switches frequently release guidelines for their safe and sound configuration (cf. documents mentioned in Chapter 7).

8.1 Technical Recommendations

The recommendations presented in this subsection should be considered as guidance to technical staff such as operators or administrators. The implementation of the listed measures should be prioritised by the results of risk assessments.

Recommendation 1: For Internet Infrastructure owners and electronic communications network regulatory agencies, evaluate your current level of security by understanding the assets covered (and not covered) by existing security measures.

Having a holistic view on the assets that have to be secured is the basis in making sure security measures are applied effectively. So, the first step for each Internet infrastructure owner and electronic communications network regulatory agency is to start with an analysis of existing (and planned) assets in order to understand existing or potential threats.

Internet infrastructure owners should evaluate how current security measures mitigate the threats applicable to these identified assets. In particular, they could focus on Important Specific Threats linked to Routing, DNS and Denial of Service.

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *Administrators, Operators*

Recommendation 2: For Internet infrastructure owners, evaluate the application of adapted good practices in a focused manner.

Internet infrastructure owners should generally consider making use of recommendations of community driven, well-known open standards organisations such as IETF, Internet Society, Euro-IX or RIPE. They should also take vendor-specific recommendations into account to secure the organisation's hardware and software infrastructure throughout its entire life cycle.

Internet infrastructure owners need to define which measures to apply, and how to deploy them, in order to enhance the security of individual assets and of their entire system. For instance, they could prioritise specific security measures by giving more attention to the threats they face. For that purpose, they can rely on monitoring for example.

This applies to recommendations for technical details such as device configuration or software development as well as to organisational structures like the securing of business processes and performing risk assessment.

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *System configuration, Essential addressing protocols, Administrators, Operators*

Recommendation 3: For Internet infrastructure owners, cooperate with the community to exchange on threats and promote the application of good practices as mitigation measures.

Internet infrastructure owners need to establish better coordination in the area of Internet infrastructure security. Security processes and measures at a local, as well as on a larger scale, require coordination for effective mitigation on technical and operational levels. It also includes the assignment of responsible personnel and the building of regional, national, and multi-national communities of trust and information exchange platforms.

The exchange of confidential information can occur:

- On the basis of trust;⁷⁵ since the disclosure of incidents may have a negative impact on the reputation;
- Through regulation and legal obligations, as it exists through Article 13a of EU Directive 2009/140/EC;⁷⁶
- Via Information Sharing and Analysis Centres (ISAC).⁷⁷

It is also important to commit to participating, this ensures that other organisations experience the application in practice and may follow suit.

Moreover, such cooperation is beneficial to enhance the security level of the Internet. It shall help understanding the pre-requisites and challenges linked to the deployment of good practices by

⁷⁵ http://www.terena.org/news/fullstory.php?news_id=2666

⁷⁶ "Article 13a of EU Directive 2009/140/EC", <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electronic%20Communications%202013%20NO%20CROPS.pdf>

⁷⁷ "Financial Services Information Sharing and Analysis Center", <https://www.fsisac.com>

Internet infrastructure owners. It can also lead to the development of new (community-driven) good practices to cover emerging threats.

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *System configuration, Essential addressing protocols, Administrators, Operators*

Recommendation 4: For users deploying good practices guides, report on their implementations, assets covered and gaps found.

For organisations that want to apply existing good practices it is of great help if the good practice guides shows a list of successful implementations. If this list contains well-known names, the importance of the good practices is stressed. Also, the organisation that is about to apply the security measures described in the good practices can contact the other organisations that already successfully applied the security measures in order to discuss open questions.

For that purpose, it is recommended that organisations deploying good practices report to their authors inconsistencies, for example cases where the good practice is not directly applicable due to a very specific Internet infrastructure. In relation with recommendation 3, this exchange of information can be realised through a community-driven platform.

Moreover, developers of good practices could also highlight the assets covered by the security measures described and which gaps still exist. This helps organisations applying the security measures described in the good practice guide to easily understand which assets are covered and which assets are still untouched.

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *System configuration, Administrators, Operators*

Recommendation 5: Words matter: Ensure the right use of terms and definitions.

For a community within the same domain it is advisable to make use of the same terminology. This will improve the comprehensibility of written material and help in discussing related topics. Among others the RFC 4949⁷⁸ provides a set of security terms and definitions.

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *Administrators, Operators*

⁷⁸ <http://tools.ietf.org/html/rfc4949>

8.2 Organisational Recommendations

The organisational recommendations are to be understood and implemented by responsible management staff and focus on defining operational procedures and processes.

Recommendation 6: For Internet infrastructure owners, use proper risk assessment methods to understand vulnerable assets in your Internet infrastructure and prioritise your protection actions.

It is advisable that Internet infrastructure owners prioritise actions to protect their Internet infrastructure. However, only a risk assessment will expose reliable figures about the probability of potential loss, also denoted as risk. Identified gaps may be covered by implementing measures presented in the chapter on good practices (cf. Section 7).

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *System configuration, Essential addressing protocols, Administrators, Operators, Administrators, Operators*

Recommendation 7: Build an information and communication technology security awareness and training program.

An ICT training program is crucial for the security of the Internet infrastructure in every company. The content and scope of the program must be tied to existing security directives and established policies. Further, it must cover all positions within a company and should distinguish between general security training in order to raise awareness, and special programs tailored to the specific roles of experts. A basic understanding of security can be obtained with a comprehensive certification scheme. Nonetheless, it is important to state that although certification is a valuable building block, it is indeed not a solution to absolutely rely on. Frequent activities ensure practice readiness and should include extensive debriefing sessions to discuss the lessons learned.

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *System configuration, Essential addressing protocols, Administrators, Operators*

Recommendation 8: Internet infrastructure owners shall commit third-party vendors to apply security measures.

Internet infrastructure owners should recommend that the vendor follows certain rules, recommendations, or certifications in line with their architecture or business model. Those rules should be defined as a part of the asset owner's risk assessment under the supervision of the company's security personnel. This ensures an extended impact of recommendations and will improve security sustainable.

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*

- Denial of Service / Flooding: *System configuration, Essential addressing protocols, Administrators, Operators*

Recommendation 9: Stay current on any updates.

Stay current on protocol and specification updates, and evaluate the prompt implementation within your own infrastructure and systems. This can be achieved through participation at conferences and workshops or simply by subscribing to mailing lists or journals. Practical experience shows that in many cases updated protocols or specification are available but simply not, or only inadequately, implemented.

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *System configuration, Essential addressing protocols, Administrators, Operators*

9 Conclusion

This Threat Landscape and Good Practice Guide for Internet Infrastructure shall permit Internet infrastructure owners to secure their assets against important and emerging threats.

For that purpose, this study has classified assets and threats of the Internet infrastructure into mind maps. It has highlighted the assets involved in Important Specific Threats, which comprise Routing threats, DNS threats, Denial of Service and Generic threats. Moreover, threats agents, who are at the origin of the threat, have also mapped for every threat type.

For every Important Specific Threat, trends are evaluated, based on public information: the threat level is globally increasing at the exception of DNS threats, in decrease (although, the number of attacks remains elevated).

For each Important Specific Threat, the study details a list of existing good practices that aim at mitigating these threats. The good practices are associated with the list of assets covered and those uncovered.

Based on the list of uncovered assets, a gap analysis is performed. It enhances the lack of good practices addressing the threats linked to human resources (administrators and operators), system configuration and essential addressing protocols.

Finally, a list of five technical and four organisational recommendations is proposed to improve the security of the Internet infrastructure. Moreover, Internet infrastructure owners can reuse or adapt the tools proposed in this study (e.g. mind maps, matrix linking threats and assets, matrix linked threats and threat agents) to evaluate their level of exposure to current threats. They can also evaluate (or improve) their current security measures for every assets linked to these threats.

Annex A: Description of Internet Infrastructure Assets

This section describes the different groups of the “Internet Infrastructure Assets” taxonomy, represented by the mind map in Figure 3 and detailed in Annex B. The description does not cover the full mind map, as this would be going beyond the purpose of this study. This study focus on the assets of the mind map which are of special interest for the threat analysis and the best common practice coverage.

Protocols

A protocol is a set of digital rules for data exchange within or between computer systems. Protocols are valuable assets for the Internet infrastructure because they allow meaningful communication between different computer systems:

- *Essential addressing protocols:* Essential addressing protocols (e.g., ARP, IPv4, IPv6, DNS) are used to address one or a group of computer systems in a network. Another set of essential addressing protocols such as TCP and UDP allow addressing of a particular executable program running on a single computer system.
- *Routing protocols:* A routing protocol is a set of rules used by routers to determine the most appropriate paths into which they should forward packets towards their intended final destinations. To route data within an Internet provider’s own network protocols such as RIP, MPLS, or OSPF are typically used. Between different Internet providers the routing protocol BGP is usually employed to exchange routing paths. Routing protocols rely on essential addressing protocols.
- *Connectivity protocols:* If different essential addressing protocols are used and communication between these different worlds should be provided, connectivity protocols can be applied. For instance, to enable IPv6-based communication on an IPv4 network, the protocol 6to4 can be used. Another example is NAT, which allows the hiding of a network of unroutable IPv4 addresses behind a single IP address and enabling limited Internet connectivity.
- *Application protocols:* Executable programs define their own task dependent protocols (e.g., HTTP, FTP, or SMTP) to exchange data.

Security protocols: Security protocols are a particular set of digital rules that ensure the protection of data by applying cryptographic primitives such as signing and encrypting. Security protocols typically wrap existing application protocols (e.g., HTTPS, FTPS, IMAPS) or enhance existing protocols (e.g., IPsec, DNSSec).

Services

A service, with regards to the Internet infrastructure, refers to an abstract combination of other functionalities utilizing other assets in order to fulfil a defined task. Services are important, as without services the concept of the Internet is of no use. Services can be structured as follows:

- *Essential addressing:* For the different layers of the Internet Protocol Stack addressing concepts exist which are described in the following section:
 - *Link layer addressing:* For the link layer typically the Ethernet protocol is used which relies on so-called MAC addresses. The MAC addresses are distinct numbers assigned to networking hardware devices. Ranges of numbers are managed and assigned to hardware manufactures by the IEEE.
 - *Internet Protocol addressing:* The Internet Protocol is the principal communication protocol of the Internet. A unique address is assigned to any communication participant in order to transmit information through the entire Internet to a defined

destination. The address space is maintained by IANA, which gives address space to the various “Regional Internet Registries” (RIRs) (cf. Routing). The RIRs themselves split up their given address spaces and distribute them to the “Local Internet Registries” (LIRs). LIRs allocate their customers (e.g., end users or companies) the given address space in the Internet.

- Transport protocol addressing: The transport protocols provide end-to-end communication services to software programs of dissimilar hosts. It adds an abstraction layer onto the Internet Protocol addressing and distinguishes between different applications on the same host by assigning unique numbers, so-called ports. These port numbers are maintained by the IANA. Prominent protocols are TCP and UDP.
- Domain Name System: The domain name system is responsible for translating easily-memorable domain names (e.g., enisa.europa.eu) to numeric Internet Protocol addresses. Domain names are managed by domain name registrars, which are organised under a hierarchy headed by the IANA.
- Addressing Unit: In general, for addressing resources in the Internet, the so-called Uniform Resource Indicators (URIs) are used. The syntax of URIs is as follows: It starts with a protocol of how the resource can be accessed, followed by a colon and two slashes, followed by an Internet Protocol address or a domain name, followed by an optional colon and port number, and finishes with the full path to the resource. For example:
`http://www.enisa.europa.eu/@@search?SearchableText=enisa`
- *Routing*: Routing is the process of selecting best paths between two points of communication in a network. Administrative instances of the routing service, which are often called "Regional Internet Registries" (e.g., RIPE NCC, LACNIC, APNIC, ARIN, AfriNIC) map network identifiers, so-called autonomous system numbers, to organizations (e.g., companies or government entities) which are participating on the Internet.
- *Applications*: Application communication, such as electronic mail or file transfer, relies on protocols that are implemented by software (e.g., executable programs) in order to provide a service to end users or machines.
- *Security*: Security services aim to maintain the security goals confidentiality, integrity, availability, authenticity, and non-repudiation.

Hardware

Hardware is defined as physical components of computer systems such as machines or wiring. Without hardware no software can be executed or information stored, hence hardware is a valuable asset. For the Internet infrastructure they are grouped into three categories:

- *Network devices*: Equipment facilitating the use of computer networks are called network devices. For instance, switches forward frames based on layer 2 addresses, routers utilise layer 3 addresses to forward packets, firewalls filter network data based on pre-defined rules, and bridges combine different network segments.
- *Servers*: A server is a computer system that provides services to other computers or users by running executable programs.
- *Personal terminals*: A personal terminal is an electronic hardware device used for communication with other computer systems.

Interconnection

As the Internet is a network of different large computer networks, the assets providing interconnection functionality are very valuable. Two different kinds of organisations can be defined:

- *Generic Internet provider*: A generic Internet provider is an organization that provides services for accessing the Internet. Generic Internet providers may be organised in various forms, such as commercial, community owned, non-profit, or otherwise privately owned. Internet providers specialise in the kind of service they provide: Data centre operators and server providers run data centres and rent space or servers respectively. Internet access providers employ a range of technologies (e.g., Wi-Fi, copper or fibre cables) to connect users to their network. Backbone providers usually run a larger network and provide Internet connectivity to Internet access providers, data centres, and server providers.
- *Internet exchange point*: An Internet exchange point consists mainly of one or more switches to interconnect different Internet providers, in order to exchange Internet traffic between their networks.

Software

Software is a generic term for collections of computer data and instructions in order to manage information and store new information, provide access to information, and process it. Software is of special importance because hardware is often useless without software, and services are built on top of software. Software can be structured as follows:

- *Operating systems*: Operating systems provide the basic non-task-specific function of computers. Operating systems are responsible for controlling, integrating, and managing the individual hardware components of a computer system by relying on device drivers and firmware so that other task-specific software and users can easily interact with the system.
- *Device drivers*: A device driver is a computer program that operates or controls a particular type of device that is attached to or integrated into a computer, by talking to the device's firmware. Device drivers are often considered to be part of an operating system because they interact closely with it.
- *Firmware*: The term firmware describes a combination of persistent memory, program code, and data stored within it. The persistent memory is part of a particular hardware component (e.g., a line card of a router). A device driver usually communicates with the firmware of a particular hardware component in order to control or manage it.
- *Executable programs*: A piece of software that is designed to fulfil a particular purpose is called an executable program. Executable programs require an operating system in order to be executed.

Infrastructure

The term infrastructure denotes the basic physical structures and facilities (e.g., buildings and cables) needed for the operation of the Internet. In order to build a worldwide network of networks, the so-called Internet, the supporting infrastructure is crucial. It can be grouped as follows:

- *Cabling and linking*: Cables and other links are used to interconnect networking devices or networks. Customarily, those connections are either wired or wireless links. Miscellaneous types of cable links like copper or fibre are used depending on the network bandwidth, size, or performance requirements and contingent upon environmental constraints such as undersea cables, underground cables, or above-ground cables. If the deployment of physical connections is not feasible or inefficient, wireless links can be employed instead. Such technologies include Wi-Fi, WIMAX, or LTE.

- **Buildings:** Buildings are facilities that house assets such as hardware, software, and interconnection. This ranges from special purpose facilities like landing points where undersea cables land ashore, to multi-purpose data centres that are used to house all kinds of hardware and infrastructure.
- **Power supply:** A power supply is a system that supplies electrical energy.
- **Cooling systems:** A cooling system regulates the temperature and humidity properties of air in order ensure the proper operation of computer systems.
- **Physical security:** Physical security refers to measures that deny unauthorised access to infrastructure. These measures include but are not limited to fences, walls, and doors.

Information

Information is perception derived from the collection of data. Information is a valuable asset because systems (e.g., software, hardware, services) and human resources depend on it to make reasonable decisions. The information assets identified are grouped as follows:

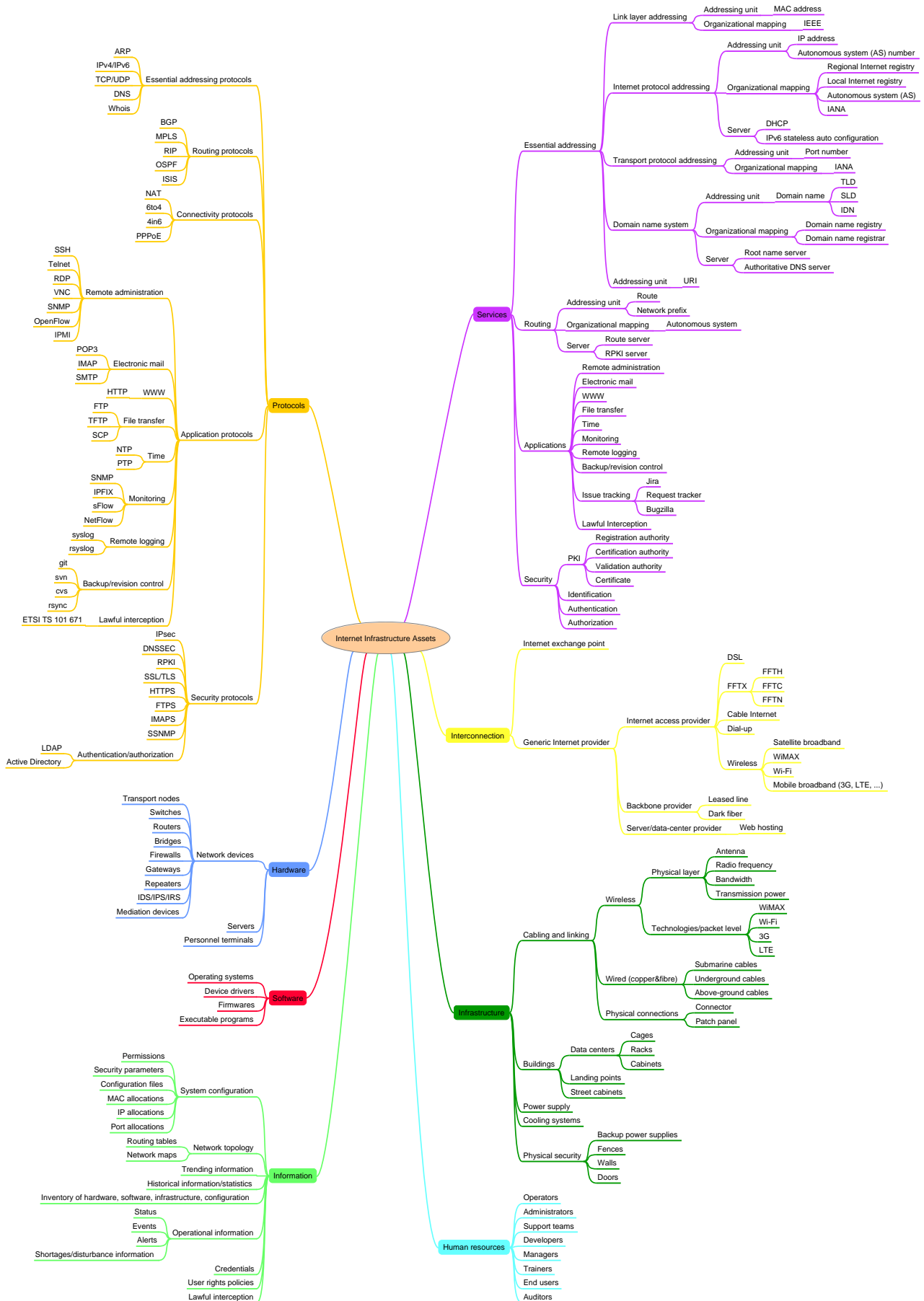
- **Inventory of hardware, software, infrastructure, information:** A list of detailed information about hardware, software, infrastructure components, and important information such as configurations. The detailed information may contain the version of the item, the place where it is located, and invoices, but is not limited to this.
- **Historical information/statistics:** Historical information is information which was collected in the past and can be accessed in the present. Some kinds of historical information may only be collected in accordance with the law, other kinds are collected in order to create statistics on such topics as usage or who has accessed the resource.
- **Trending information:** Attempting to identify trends in the information collected is often used to predict the future based on past events or behaviour.
- **Network topology:** Network topology is the arrangement of various components (e.g., routers, switches, firewalls, servers) of a computer network. Such details may be filed as network maps or routing tables.
- **System configuration:** System configuration describes how different components (e.g., software, hardware) of a system (e.g., software, hardware, services) are configured, connected, and interoperate in order to achieve a certain goal. For instance, the router MAC and IP addresses configure its network subsystem.
- **Operational information:** Information that is needed to operate a system is called operational information. Operational information comprises the status of a system, measures for certain metrics, events when the state of a system changes, alerts when a certain threshold for particular metric is reached, and information about shortages or disturbances.
- **Credentials:** A credential is an attestation of authority issued to a machine or person by a third party. It might be physical, such as keys and passports, or virtual (e.g. usernames and passwords, PINs).
- **User rights policies:** User rights policies define the permissions of groups of users (e.g., administrators, operators) to certain information (such as computer systems, executable programs, information).
- **Lawful interception:** Lawful interception is obtaining access to communications network data pursuant to lawful authority for the purpose of analysis, evidence, or surveillance.

Human Resources

This section defines the personnel which are considered to be a significant asset of the Internet infrastructure in terms of skills and abilities.

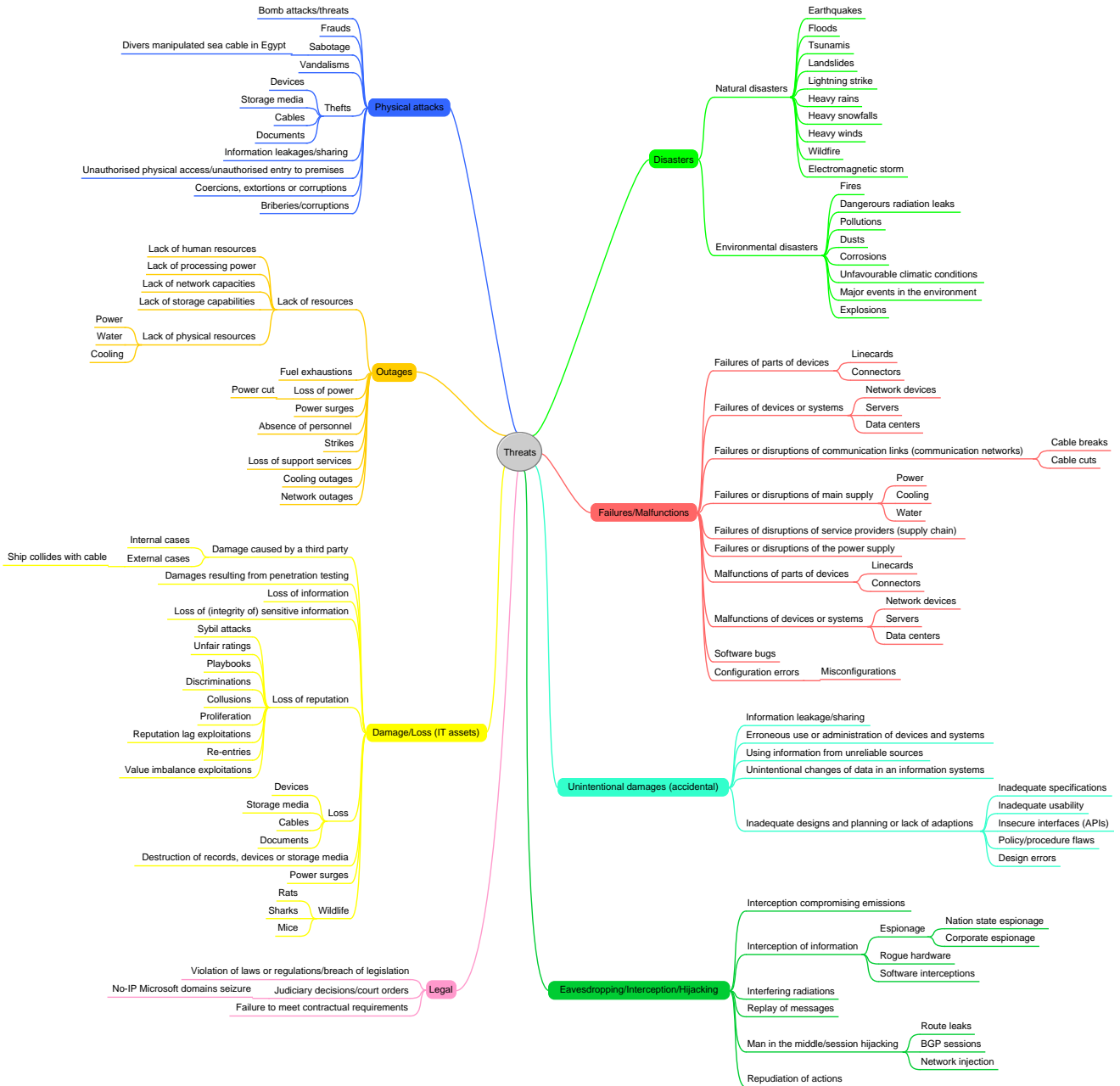
- *Administrators*: A person that is responsible for setting up, configuring, monitoring, and maintaining a system (e.g., server, router).
- *Operators*: A person or a company that runs software, machines, or systems.
- *Support team*: A person or a group that provides help on the usage, configuration, or fault detection of a system or service.
- *Developers*: A person concerned with researching, designing, implementing, and testing of systems or software.
- *Managers*: A person that is responsible for controlling or administering an organization or group of staff (e.g., administrators, operators, developers).
- *Trainers*: A person that educates another person on a specific topic.
- *Auditors*: A person that validates and verifies that a person, process, or system, behaves, runs, or is being used in an environment as previously defined.
- *End users*: A person who actually uses a particular product or service.

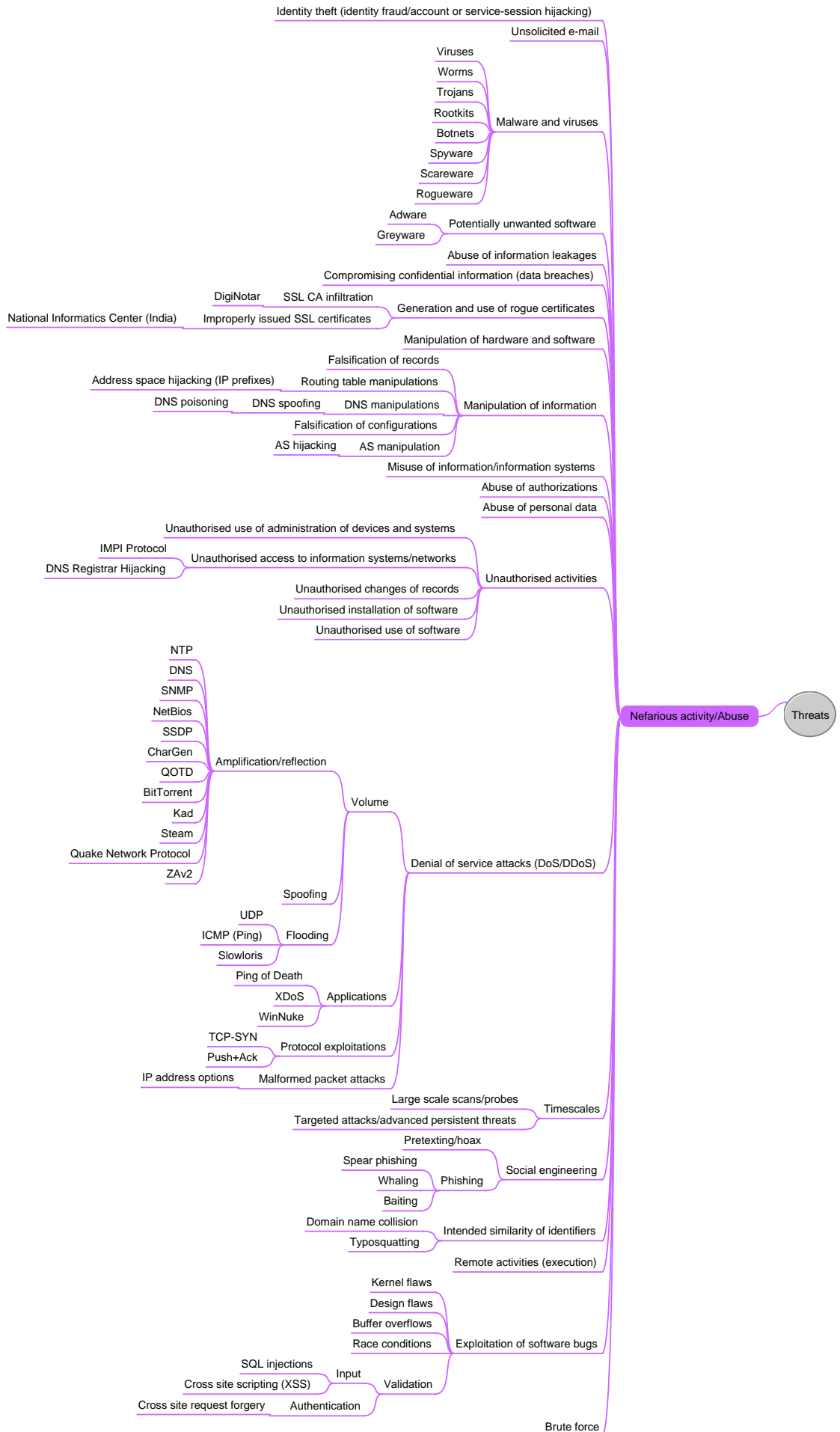
Annex B: Detailed Mind Map for Internet Infrastructure Assets



Annex C: Threat Mind Map

The threat mind map is divided into two parts for enhanced readability:





Annex D: Association between threats and assets

Threat types	Threats	Asset types
Physical attacks		
	Bomb attack/threats	Hardware, Infrastructure, Human resources
	Fraud	Human resources
	Sabotage	Hardware, Infrastructure
	Vandalism	<i>Ditto</i>
	Thefts	<i>Ditto</i>
	Information leakages/sharing	Information, Infrastructure, Interconnection
	Unauthorised physical access/unauthorised entries to premises	Hardware, Infrastructure
	Coercions, extortions or corruptions	Hardware, Infrastructure
	Briberies/corruptions	Human resources
Disasters		
	Natural disasters	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Environmental disasters	<i>Ditto</i>
Failures/Malfunctions		
	Failures of parts of devices	Protocols, Hardware, Software, Information, Services
	Failures of devices or systems	<i>Ditto</i>
	Failures or disruptions of communication links (communication networks)	<i>Ditto</i>
	Failures or disruptions of main supply	Protocols, Hardware, Software, Information, Services, Interconnection, Infrastructure
	Failures or disruptions of service providers (supply chain)	Protocols, Hardware, Software, Information, Services
	Failures or disruptions of the power supply	Protocols, Hardware, Software, Information, Services, Interconnection, Infrastructure
	Malfunctions of parts of devices	<i>Ditto</i>
	Malfunctions of devices or systems	<i>Ditto</i>
	Software bugs	Protocols, Software, Information, Services
	Configuration errors	Protocols, Hardware, Software, Information, Services
Outages		
	Lack of resources	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources

Threat types	Threats	Asset types
	Fuel exhaustions	Hardware, Infrastructure, Human resources
	Loss of power	<i>Ditto</i>
	Power surges	<i>Ditto</i>
	Absence of personnel	<i>Ditto</i>
	Strikes	Human resources
	Network outages	Hardware, Software, Information, Services
	Cooling outages	Hardware, Infrastructure
Unintentional damages (accidental)		
	Information leakage/sharing	Hardware, Software, Information, Services, Interconnection
	Erroneous use or administration of devices and systems	Protocols, Hardware, Software, Information, Services
	Using information from unreliable sources	Protocols, Hardware, Software, Information, Services
	Unintentional change of data in an information systems	Protocols, Hardware, Software, Information, Services
	Inadequate designs and planning or lack of adaptations	Protocols, Hardware, Software, Information, Services, Interconnection, Infrastructure
Damage/Loss (IT assets)		
	Damage caused by a third parties	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Damages resulting from penetration testing	Software, Information, Services
	Loss	Protocols, Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Loss of reputation	Interconnection, Human resources
Nefarious activity/Abuse		
	Identity theft (identity fraud/account or service-session hijacking)	Hardware, Software, Information, Services, Infrastructure, Human resources
	Unsolicited e-mail	Hardware, Software, Services
	Malware and viruses	Hardware, Software, Information, Services
	Potentially unwanted software	<i>Ditto</i>
	Abuse of information leakages	<i>Ditto</i>
	Compromising confidential information (data breaches)	Protocols, Hardware, Software, Information, Services
	Generation and use of rogue certificates	Hardware, Software, Information, Services, Human resources

Threat types	Threats	Asset types
	Manipulation of hardware and software	Protocols, Hardware, Software, Information, Services
	Manipulation of information	Protocols, Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Misuse of information/information systems	Protocols, Hardware, Software, Information, Services, Interconnection
	Abuse of authorizations	Protocols, Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Abuse of personal data	Human resources
	Unauthorised activities	Protocols, Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Denial of service attacks (DoS/DDoS)	Hardware, Software, Information, Services
	Timescales	<i>Ditto</i>
	Social engineering	Human resources
	Intended similarity of identifiers	Information, Services
	Remote activities (execution)	Software, Information, Services
	Exploitation of software bugs	Protocols, Software, Information, Services
	Brute force	<i>Ditto</i>
Eavesdropping/ Interception/Hijacking		
	Interception compromising emissions	Protocols, Software, Information, Services
	Interception of information	Protocols, Software, Information, Services
	Interfering radiations	Hardware, Interconnection, Infrastructure, Human resources
	Replay of messages	Software, Information, Services
	Man in the middle/session hijacking	Software, Information, Services
	Repudiation of actions	Interconnection, Human resources
Legal		
	Violations of law or regulation/breaches of legislation	Software, Information, Interconnection, Human resources
	Judiciary decisions/court orders	<i>Ditto</i>
	Failure to meet contractual requirements	<i>Ditto</i>

Annex E: Threat Details

The present table is based on a ENISA general purpose tool to capture a threat taxonomy and relevant threat details.

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
Physical attacks					
	Bomb attack/threats		Cyber terrorists, employees, nation states, cyber criminals		
	Frauds		Cyber terrorists, employees, cyber criminals, corporations		
	Sabotage		Cyber terrorists, employees, corporations, nation states		
	Vandalism		Employees, cyber criminals		
	Thefts	Theft of physical company property such as devices, media, or documents.	Employees, cyber criminals	Increasing	
	Information leakages/sharing		Employees, corporations	Increasing	
	Unauthorised physical access/unauthorised entries to premises		Ditto		
	Coercions, extortions or corruptions		Cyber terrorists, cyber criminals, employees, corporations, nation states		
	Briberies/corruptions		Ditto		

⁷⁹ “Arbor Networks ATLAS Report”, <http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5242-arbor-networks-reports-the-most-volumetric-ddos-attacks-ever-in-the-first-half-of-2014>

⁸⁰ “Mandiant Trends 2014”, <https://www.mandiant.com/resources/mandiant-reports/>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
Disasters	Natural disasters	Earthquakes			
		Floods			
		Landslides			
		Lightning strike			
		Heavy rains			
		Heavy snowfalls			
		Heavy winds			
		Wildfire			
		Electromagnetic storm			
		Environmental disasters			
	Fires				
	Dangerous radiation leaks				
	Pollutions				
	Dusts				
	Corrosions				
	Unfavourable climatic conditions				
	Major events in the environment				
	Explosions				
Failures/ Malfunctions			Employees, corporations		
	Failures of parts of devices				
	Failures of devices or systems				

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
	Failures or disruptions of communication links (communication networks)				
	Failures or disruptions of main supply				
	Failures or disruptions of service providers (supply chain)				
	Failures or disruptions of the power supply				
	Malfunctions of parts of devices				
	Malfunctions of devices or systems				
	Software bugs				
	Configuration errors	False, insufficient, or insecure configuration of systems, also referred to as misconfiguration.			Misconfigured Apache sites expose [...] private data. ⁸¹
Outages					
	Lack of resources	Lack of physical resources as well as processing power, network capacity, or human resources.	Employees, corporations		
	Fuel exhaustions		Ditto		
	Loss of power		Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states		
	Power surges		Ditto		
	Absence of personnel		Employees, corporations		

⁸¹ <http://arstechnica.com/security/2012/11/misconfigured-apache-sites-expose-user-passwords-other-private-data/>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
	Strikes		Employees		
	Network outages		Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states		
	Cooling outages		Ditto		
Unintentional damages (accidental)			Employees, corporations	Increasing	
	Information leakage/sharing			Increasing	
	Erroneous use or administration of devices and systems				
	Using information from unreliable sources				
	Unintentional change of data in an information systems				
	Inadequate designs and planning or lack of adaptations	Inadequate design includes inadequate specifications, usability, and resulting insecure API or design errors.			
Damage/Loss (IT assets)				Increasing	
	Damage caused by a third parties		Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nation states		
	Damages resulting from penetration testing		Corporations		

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
	Loss	Loss of company property such as devices, media, power, or documents. Includes loss of information.	Online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states	Increasing	Visualization. ⁸² Verizon 2014 data breach investigation report. ¹³ Anatomy of a Data Breach. ⁸³
	Loss of reputation	Loss of reputation includes attacks to fore the loss and unintentional or even deserved loss. (Sybil attacks, discrimination, ratings, collusion, proliferation, or re-entry)	Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states		
Nefarious activity/Abuse					
	Identity theft (identity fraud/account or service-session hijacking)		Online social hackers, hacktivists, script kiddies, cyber criminals, insider, nation states	Increasing	
	Unsolicited e-mail		Online social hackers, hacktivists, script kiddies, cyber criminals	Increasing	
	Malware and viruses	Malware can be further categorised in groups such as virus, worm, trojan, rootkit, botnets, spyware, scareware, or rogueware.	Online social hackers, hacktivists, script kiddies, cyber criminals, nation states	Increasing	TDL/TDL4/TDSS malware (virus, trojan, rootkit, botnet) massive infection of high-end malware. ⁸⁴ Blackhole exploit kit. ⁸⁵ Java vulnerabilities exploited for intrusion in ~90% of infections. ⁸⁶
	Potentially unwanted software	Has, in contrast to malware, legitimate functionality to conceal	Online social hackers, hacktivists, script kiddies, cyber criminals,		

⁸² <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

⁸³ <http://about-threats.trendmicro.com/us/webattack/110/Anatomy+of+a+Data+Breach>

⁸⁴ <http://www.viruslist.com/de/analysis?pubid=200883742>

⁸⁵ <http://www.avgthreatlabs.com/virus-and-malware-information/info/blackhole-exploit-kit/>

⁸⁶ <http://securelist.com/analysis/kaspersky-security-bulletin/58265/kaspersky-security-bulletin-2013-overall-statistics-for-2013/>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
		true goals. Installed unintentionally, includes adware and greyware.	employees		
	Abuse of information leakages		Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nations states	Increasing	
	Compromising confidential information (data breaches)		Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nations states, employees	Increasing	
	Generation and use of rogue certificates	SSL CA infiltration or improperly issued SSL certificates.	Online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nations states		
	Manipulation of hardware and software		Online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nations states		
	Manipulation of information		Online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nations states		
		Falsification of records			
		Routing table manipulation		Increasing	Indosat routing leak involving >320k non-Indonesian BGP routes. For some Akamai prefixes (networks), the Indosat hijack was essentially complete. ⁸⁷ Traffic inception has certainly been a hot topic in 2013. About 1,500 individual IP blocks have been hijacked, in events lasting

⁸⁷ <http://www.renesity.com/2014/04/indonesia-hijacks-world/>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
					<p>from minutes to days, by attackers working from various countries.⁸⁸</p> <p>China's government diverted 15% of the Internet's traffic for eighteen minutes in April 2010.⁸⁹</p> <p>On Sunday, 24 February 2008, Pakistan Telecom started an unauthorised announcement of the prefix 208.65.153.0/24. One of Pakistan Telecom's upstream providers, PCCW Global forwarded this announcement to the rest of the Internet, which resulted in the hijacking of YouTube traffic on a global scale.⁹⁰</p> <p>Since February 2013, they have observed 38 distinct events in which large blocks of traffic have been improperly redirected to routers at Belarusian or Icelandic service providers.⁹¹</p>
		DNS manipulation		Decreasing	<p>Attacking the DNS.⁹²</p> <p>Kaminsiky attack.⁹³</p> <p>Protecting against DNS cache poisoning attacks.⁹⁴</p> <p>The collateral damage of Internet censorship by DNS injection.⁹⁵</p>

⁸⁸ <http://www.renesys.com/2013/11/mitm-internet-hijacking/>

⁸⁹ <http://www.renesys.com/2010/11/chinas-18-minute-mystery/>

⁹⁰ <http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

⁹¹ <http://www.menog.org/presentations/menog-13/194-MENOG13-Hijack.pdf>

⁹² <https://www.iana.org/about/presentations/davies-viareggio-entropyvuln-081002.pdf>

⁹³ <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>

⁹⁴ <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5634454>

⁹⁵ <http://dl.acm.org/citation.cfm?doid=2317307.2317311>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
		Falsification of configuration			
		AS manipulation			Manipulation of AS numbers or the numbering system itself.
	Misuse of information/information systems		Online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states		
	Abuse of authorizations		Online social hackers, hacktivists, script kiddies, cyber criminals, employees		
	Abuse of personal data		Ditto		
	Unauthorised activities		Employees		
		Unauthorised use of administration of devices and systems			
		Unauthorised access to information system/network			
		Unauthorised changes of records			
		Unauthorised installation of software			
		Unauthorised use of software			
	Denial of service attacks (DoS/DDoS)		Online social hackers, hacktivists, script kiddies, cyber criminals	Increasing	41% of all organizations globally suffered a DDoS attack over the last year. ⁹⁶ Multiple responders report very large DDoS attacks above the 100Gbps threshold. Application-layer attacks were seen by almost all respondents. Attacks targeting

⁹⁶ <http://www.computing.co.uk/ctg/news/2352764/ddos-attacks-hit-41-per-cent-of-organisations-in-the-past-year>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
					<p>encrypted Web services (HTTPS) – up 17 percent over last year.⁹⁷</p> <p>18% increase in total DDoS attacks (Q1 2014 to Q4 2013). 39% increase in average attack bandwidth. 35% increase in infrastructure attacks (layer 3+4). 114% increase in average peak bandwidth. 36% decrease in application (layer 7) attacks. 24% decrease in average attack duration: 23 vs. 17 hours.⁹⁸</p> <p>In Q1 2014, 41% of observed attacks are coming out of China (compared to 43% in Q4 2013). Universal Plug&Play (UPnP) is the new famous attack port (12% of attack traffic). Slight decline in the number of attacks compared to Q4 2013: 283 (down 20%), but an 27% increase compared to Q1 2013.⁹⁹</p> <p>One of World’s Largest Websites Hacked: Turns Visitors into “DDoS Zombies”¹⁰⁰.</p>
		Volume			<p>CloudFlare 400 Gbps NTP Amplification DDoS Attack.¹⁰¹</p> <p>Repeat attacks hit two thirds of DDoS victims. DDoS amplification attacks still a daunting challenge. Increase in government targets, decrease in bank targets. Increase in legitimate online gaming server targets.¹⁰²</p>
		Application			

⁹⁷ <http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf>

⁹⁸ <http://www.prolexic.com/kresources/attack-report/prolexic-quarterly-global-ddos-attack-report-q114/A4-Q12014-Global-Attack-Report.pdf>

⁹⁹ <http://www.akamai.com/dl/akamai/akamai-soti-a4-q114.pdf>

¹⁰⁰ <http://www.incapsula.com/blog/world-largest-site-xss-ddos-zombies.html>

¹⁰¹ <http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack>

¹⁰² <http://en.nsfocus.com/SecurityReport/NSFOCUS DDoS Threat Report 2013.pdf>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
		Protocol exploitation			
		Malformed packet attack			
	Timescales				
		Large scale scan/probe	Online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nation states	Increasing	
		Targeted attacks/advanced persistent threat	Online social hackers, hacktivists, script kiddies, cyber criminals, nation states	Stable	
	Social engineering		Online social hackers, hacktivists, script kiddies, cyber criminals		Social engineering: The art of human hacking. ¹⁰³
		Phishing		Increasing	
		Pretexting/hoax			
	Intended similarity of identifiers		Online social hackers, hacktivists, script kiddies, cyber criminals		
		Domain name collision			Name Collision in the DNS. ¹⁰⁴
		Typosquatting, registering common typo domains			Typosquatting - what happens when you mistype a website name? ¹⁰⁵
	Remote activities (execution)		Online social hackers, hacktivists, script kiddies, cyber criminals, nation states		
	Exploitation of software bugs		Ditto		
		Kernel flaw			
		Design flaw			

¹⁰³ Christopher Hadnagy, "Social engineering: The art of human hacking", John Wiley & Sons, 2010.

¹⁰⁴ <https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf>

¹⁰⁵ "Typosquatting - what happens when you mistype a website name?", <https://nakedsecurity.sophos.com/typosquatting/>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
		Buffer Overflow			
		Race Condition			
		Insufficient validation		Increasing	
	Brute force	A trial-and-error method used to obtain information such as login credentials, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.	Ditto		Brute force RDP attacks depend on your mistakes. ¹⁰⁶ Kaspersky: Online social hackers, hacktivists, script kiddies try to take over PCs running remote desktop software. ¹⁰⁷
Eavesdropping /Interception /Hijacking					
	Interception compromising emissions		Online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nation states		
	Interception of information	Interception of information through espionage, rogue hardware, or direct software interception.	Online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states		Snowden says NSA engages in industrial espionage. ¹⁰⁸ GCHQ and NSA Targeted Private German Companies. ¹⁰⁹
	Interfering radiations		Cyber terrorists, corporations, nation states		
	Replay of messages		Online social hackers, hacktivists, script kiddies, cyber criminals,		

¹⁰⁶ <http://www.zdnet.com/brute-force-rdp-attacks-depend-on-your-mistakes-7000031071/>

¹⁰⁷ <http://www.myce.com/news/kaspersky-online-social-hackers-hacktivists-script-kiddies-try-to-take-over-pcs-running-remote-desktop-software-72132/?PageSpeed=noscript>

¹⁰⁸ <http://www.reuters.com/article/2014/01/26/us-security-snowden-germany-idUSBREAOPDE20140126>

¹⁰⁹ <http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html>

Threat groups	Threat	Threat details	Threat agents	Trend ^{6, 13, 79, 80}	Comments, examples
			employees		
	Man in the middle/session hijacking	Examples are route leaks or hijacked BGP sessions.	Online social hackers, hacktivists, script kiddies, cyber criminals, corporations, nation states		NANOG49 talk. ¹¹⁰ Practical Defenses Against BGP Prefix Hijacking. ¹¹¹
	Repudiation of actions		Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states		
Legal					
	Violations of law or regulation/breaches of legislation		Cyber terrorists, online social hackers, hacktivists, script kiddies, cyber criminals, employees, corporations, nation states		
	Judiciary decisions/court orders		Nations states		
	Failure to meet contractual requirements		Employees, corporations		

¹¹⁰ <https://www.nanog.org/meetings/nanog49/presentations/Tuesday/LRL-NANOG49.pdf>

¹¹¹ <https://web.eecs.umich.edu/~zmao/Papers/conextDefendHijack07.pdf>

Annex F: Good Practices Details

Routing Threats

AS hijacking:

- Utilise resource certification (RPKI) to provide AS origin validation. In particular RPKI is used to secure BGP through BGPsec.¹¹²

Address space hijacking (IP prefixes):

- Utilise resource certification (RPKI) to provide AS origin validation. In particular RPKI is used to secure BGP through BGPsec.^{113 114}
- Establish an Appropriate Use Policy (AUP) as explained in BCP 46, which promotes rules to secure peering¹¹⁵.
- Establish ingress filtering from the edge site to the Internet.^{112 116 117}
- Establish Unicast Reverse Path Forwarding to verify the validity of a source IP address.^{118 119}
- Establish egress filtering at the boundary router to proactively filter all traffic going to the customer that has a source address of any of the addresses that have been assigned to that customer.¹¹²
- Filter the routing announcements and implement techniques that reduce the risk of putting excessive load on routing generated by illegitimated route updates/announcements.^{112 117} For instance, Route Flap Damping (RFD) with a well-defined threshold may contribute to reducing router processing time.^{118 119}
- Registry databases such as IRR, APNIC, ARIN, and RIPE have to be subject to continuous maintenance. This shall allow usage of updated information to secure peering.^{112 120} For example, the “Route Object” field can help validating routes received from peers.^{112 121 122 123}
- Configuration updates for the routing infrastructure may only be performed by a defined authority using strong authentication.¹¹²
- Monitor the status of BGP to detect unusual behaviour such as path changes or unusual announcement.¹²³

¹¹² “A Forensic Case Study on AS Hijacking: The Attacker’s Perspective”, Sigcomm CCR 2013, <http://www.sigcomm.org/sites/default/files/ccr/papers/2013/April/2479957-2479959.pdf>

¹¹³ “Use Cases and Interpretations of Resource Public Key Infrastructure (RPKI) Objects for Issuers and Relying Parties”, RFC 6907, <http://tools.ietf.org/html/rfc6907>

¹¹⁴ “Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)”, <http://www.rfc-editor.org/bcp/bcp185.txt>

¹¹⁵ “Recommended Internet Service Provider Security Services and Procedures”, Section Network Infrastructure, <http://www.rfc-editor.org/bcp/bcp46.txt>

¹¹⁶ “BGP operations and security”, <http://tools.ietf.org/html/draft-ietf-opsec-bgp-security-04>

¹¹⁷ “RIPE Anti-Spoofing Task Force HOW-TO” (RIPE-431), <http://www.ripe.net/ripe/docs/ripe-431>

¹¹⁸ “BGP Route Flap Damping”, <http://tools.ietf.org/html/rfc2439>

¹¹⁹ “RIPE: Recommendations on Route Flap Damping”, <http://www.ripe.net/ripe/docs/ripe-580>

¹²⁰ “Collective Responsibility and Collaboration for Routing Resilience and Security”, <https://www.routingmanifesto.org>

¹²¹ “APNIC: Routing object”, http://www.apnic.net/apnic-info/whois_search/about/what-is-in-whois/IRR/routing-objects

¹²² “RIPE: Managing ROAs”, <http://www.ripe.net/lir-services/resource-management/certification/resource-certification-roa-management>

¹²³ “BGP Operations and Security”, <http://tools.ietf.org/html/draft-ietf-opsec-bgp-security-05>

Route leaks:

- Configure BGP maximum-prefix to ensure the validity of routes announced. If more prefixes are received, it is sign of an incorrect behaviour and the BGP session shuts down.^{124 125 126}
- Utilise resource certification (RPKI) to provide AS origin validation.^{113 114}

BGP session hijacking:

- Establish prefix filtering and automation of prefix filters.^{114 118 122}
- Employ AS path filtering.¹¹⁶
- Use TCP-AO (TCP-Authentication Option) to secure BGP Authentication in order to replace TCP-MD5. TCP-AO simplifies the exchange of keys.^{126 127}

DNS Threats

DNS registrar hijacking:

- Registrants must protect account credentials and define authorised users, while registrars have to provide a secure authentication process.^{128 129}
- Registrants should take advantage of routine correspondence from registrar such as change notification, billing information, or WHOIS records. Hence, registrars must provide such information.^{128 129}
- Registrants should maintain documentation to “prove registration”.¹²⁸
- Registrants should use separate identities for registrant, technical, administrative, and billing contacts. Thus, registrars need to allow a more complex user rights management.^{128 129}
- Registrars must establish an effective zone data management.¹²⁸
- Registrars should consider supporting DNSSEC.^{128 129 130}
- Registrars may monitor DNS change activities.¹²⁸

DNS spoofing:

- Deploying DNSSEC aims to secure DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity.^{131 132}

DNS poisoning:

- Deploying DNSSEC aims to secure DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity.^{130 131 132}
- Restrict zone transfers to reduce load on systems and network.¹³³

¹²⁴ “BGP Configuration best practices”, http://www.ssi.gouv.fr/IMG/pdf/NP_BGP_BCP_en.pdf

¹²⁵ https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-102.pdf (in German)

¹²⁶ “BGP Operations and Security”, <http://tools.ietf.org/html/draft-ietf-opsec-bgp-security-06>

¹²⁷ “RFC 5926: Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)”, <http://tools.ietf.org/html/rfc5926>

¹²⁸ “A Registrant’s Guide to Protecting Domain Name Registration Accounts”, <https://www.icann.org/en/system/files/files/sac-044-en.pdf>

¹²⁹ “Measures to Protect Domain Registration Services Against Exploitation or Misuse”, <https://www.icann.org/en/groups/ssac/documents/sac-040-en.pdf>

¹³⁰ “Root Name Server Operational Requirements”, <http://tools.ietf.org/html/bcp40>

¹³¹ “Good practices guide for deploying DNSSEC”, <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec>

¹³² “Detection and countermeasure of forged response cache poisoning attacks”, <http://tools.ietf.org/html/draft-fujiwara-dnsop-poisoning-measures-00>

- Restrict dynamic updates to only authorised sources in order to avoid misuse.¹³³ Such misuse include the abuse of a DNS server as an amplifier, DNS cache poisoning...
- Set up the authoritative name server as non-recursive. Separate recursive name servers from the authoritative name server.¹³³
- Allow DNS transport over TCP to support non-standard queries. Moreover, TCP may be necessary for DNSSEC.¹²⁵

Domain name collision:

- Do not use random domain names that you do not own for your internal infrastructure. For example, do not consider private domain name space as top-level domains.¹³⁴
- Preventing DNS request for internal namespaces to leak into the Internet by applying firewall policies.¹³⁵
- Use reserved TLDs such as .test, .example, .invalid, or .localhost.¹³⁵¹³⁶

Denial of Service Threats

Amplification/reflection:

- Adopt source IP address verification at the edge of Internet infrastructure (close to the origin of traffic) to prevent network address spoofing through ingress and egress filtering.¹³⁷ ¹³⁸ ¹³⁹
¹⁴⁰ ¹⁴¹
- Operators of authoritative name server operator should implement RRL (Response Rate Limiting).¹³⁷
- DNS name server operators and ISPs need to disable open recursion on name servers and may only accept DNS queries from trusted sources.¹³⁷ ¹³⁸ ¹⁴⁰

Flooding:

- Manufacturers and configurators of network equipment should take steps to secure all devices and have to keep them up-to-date.¹³⁸

¹³³ "How to Secure a Domain Name Server (DNS)",

http://csrc.nist.gov/groups/SMA/fasp/documents/network_security/NISTSecuringDNS/NISTSecuringDNS.htm

¹³⁴ "SSAC Advisory Concerning the Mitigation of Name Collision Risk",

<https://www.icann.org/en/system/files/files/sac-062-en.pdf>

¹³⁵ "Name Collision Mitigation for Enterprise Networks", Name Collision Workshop 2014,

http://namecollisions.net/downloads/wpnc14_slides_hoffman_name_collision_mitigation.pdf

¹³⁶ "Reserved Top Level DNS Names", <http://tools.ietf.org/html/rfc2606>

¹³⁷ "SSAC Advisory DNS Distributed Denial of Service (DDoS) Attacks",

<https://www.icann.org/en/system/files/files/dns-ddos-advisory-31mar06-en.pdf>

¹³⁸ "SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure",

<https://www.icann.org/en/system/files/files/sac-065-en.pdf>

¹³⁹ "Ingress Filtering for Multihomed Networks", <http://www.rfc-editor.org/bcp/bcp84.txt>

¹⁴⁰ "DNS: DNS Amplification Attacks", <https://www.us-cert.gov/ncas/alerts/TA13-088A>

¹⁴¹ "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing",

<http://www.rfc-editor.org/bcp/bcp38.txt>



TP-05-14-012-EN-N

ENISA

European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



ISBN: 978-92-9204-098-7
DOI: 10.2824/34387



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu