TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Priscila da Silva Leopoldino 201638IVCM

CYBER SANCTIONS: APPLICABILITY AND CHALLENGES IN THE EUROPEAN UNION

Master's thesis

Supervisor: Aleksi Oskar Johannes Kajander

PhD

Tallinn 2026

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Priscila da Silva Leopoldino 201638IVCM

KÜBERSANKTSIOONID: RAKENDATAVUS JA VÄLJAKUTSED EUROOPA LIIDUS

Magistritöö

Juhendaja: Aleksi Oskar Johannes Kajander

PhD

Tallinn 2026

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Priscila da Silva Leopoldino

02.04.2026

Tallinn 2026

Abstract

This study examines the operational applicability of the EU cyber sanctions framework, with a focus on the criteria set out in Regulation (EU) 2019/796 for identifying cyber-attacks with a significant effect. As cyber operations continue to evolve in scale and complexity, questions arise as to whether existing legal frameworks can be effectively applied using publicly available information.

To address this, the study adopts an incident-based stress testing approach. Three cyber-attacks affecting EU member states between 2019 and 2025 are analysed as case studies. Each case is assessed against the criteria under Article 1 and Article 2 of the Regulation using qualitative indicators derived from open-source reporting. The analysis further examines recurring operational challenges and evaluates the consistency with which individual criteria can be applied across different types of cyber operations.

The findings indicate that, while certain criteria can be operationalised with relative consistency, others remain difficult to assess due to the limited availability of reliable open-source evidence. The study also shows that the framework is more readily applicable to disruptive ransomware attacks than to large-scale data breaches, highlighting uneven applicability across incident types.

This research contributes to the field by identifying structural and evidentiary limitations in the current framework and proposing targeted clarifications to improve its operational usability. The study provides a practical perspective on how the framework performs when applied to contemporary cyber-attacks, highlighting both its strengths and constraints.

This thesis is written in English and is eighty-nine pages long, including six chapters, one figure and four tables.

Lühikokkuvõte

KÜBERSANKTSIOONID: RAKENDAVATUS JA VÄLJAKUTSED EUROOPA LIIDUS

Käesolev uuring analüüsib Euroopa Liidu kübersanktsioonide raamistiku operatiivset kohaldatavust. Olulise mõjuga küberrünnakute tuvastamiseks on keskendutud määruses (EU) 2019/796 sätestatud kriteeriumidele. Kuna küberoperatsioonid muutuvad üha ulatuslikumaks ja keerukamaks, kerkib küsimus, kas olemasolevaid õigusraamistikke saab avalikult kättesaadava teabe abil tõhusalt rakendada.

Selle lahendamiseks kasutab uuring intsidendipõhist stressitestimise lähenemisviisi. Kolme küberrünnakut, mis mõjutasid EL-i liikmesriike aastatel 2019-2025, analüüsitakse juhtumiuuringutena. Iga juhtumit hinnatakse määruse artiklis 1 ja 2 sätestatud kriteeriumide põhjal, kasutades avatud allikatel põhinevaid kvalitatiivseid näitajaid. Analüüs käsitleb ka korduvaid praktilisi väljakutseid ning hindab, kui järjepidevalt on võimalik üksikuid kriteeriume eri tüüpi küberoperatsioonide puhul rakendada.

Tulemused näitavad, et kuigi teatud kriteeriume saab suhteliselt järjepidevalt rakendada, on teiste hindamine endiselt keeruline, kuna usaldusväärsed avalikud andmed on piiratud kättesaadavusega. Samuti ilmneb, et raamistik on kergemini rakendatav lunavararünnakute puhul kui ulatuslike andmeleketega juhtumites, mis viitab ebaühtlasele rakendatavusele eri intsidentide lõikes.

Uuring panustab antud valdkonda, tuues esile praeguse raamistiku struktuursed ja tõenduspõhised piirangud ning pakkudes välja sihipäraseid täpsustusi selle praktilise kasutatavuse parandamiseks. Uuring annab praktilise ülevaate sellest, kuidas raamistik toimib tänapäevaste küberrünnakute kontekstis, tuues esile nii selle tugevused kui ka piirangud.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti kaheksakümmend üheksa lehekülge leheküljel, kuus peatükki, üks joonist, neli tabelit.

List of abbreviations and terms

Council	Council of the European Union
CDT	Cyber Diplomacy Toolbox
CERT-EU	Computer Emergency Response Team for the European Union
CFSP	Common Foreign and Security Policy
CNIL	Commission nationale de l'informatique et des libertés
EU	European Union
ENISA	European Union Agency for Cybersecurity
FRCB-IDIBAPS	Fundació de Recerca Clínic Barcelona-Institut D'investigacions Biomèdiques august Pi i Sunyer
GDPR	General Data Protection Regulation
HSE	Health Service Executive
HCB	Hospital Clínic de Barcelona
PwC	PricewaterhouseCoopers

Table of contents

List of figures

List of tables

1 Introduction

In recent years, the European Union (EU) has faced an increasing number of malicious cyber activities threatening its security, economy, and political stability. As a result, cybersecurity has become a core policy concern.

Among the policy responses developed at EU level, the Cyber Diplomacy Toolbox[1] (CDT) [1], adopted in June 2017, stands out as a significant step. The CDT provides a joint diplomatic framework aimed at preventing conflicts, mitigating cyber threats, and discouraging malicious actors from targeting the EU [1].

Building on this framework, the Council of the European Union (Council) adopted a cyber sanctions regime[2] in May 2019 under the Common Foreign and Security Policy[3] (CFSP) [2][3]. This regime establishes the legal basis for the imposition of targeted restrictive measures, commonly referred to as cyber sanctions.

The cyber sanctions framework allows the EU to impose measures against individuals and entities responsible for cyber-attacks[4] with a significant effect[5] on the Union, its member states, third countries, or international organisations.

Since its adoption, the EU has demonstrated its willingness to use this instrument.

---

[1] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017.
[2] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.
[3] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States
[4] For the purpose of this study, cyber-attacks are considered as unauthorized actions involving access to information systems, system interference, data interference, or data interception, as defined in EU Regulation (EU) 2019/769.
[5] This term is introduced in Article 1 of Regulation (EU) 2019/796. Article 2 sets out the factors determining whether a cyber-attack produces a significant effect, including scope, scale, severity of disruption, number of affected persons or member states, economic loss, economic benefit gained by the perpetrator, and the nature or scale of accessed data.

In July 2020, the EU imposed its first cyber sanctions in response to the WannaCry, NotPetya, and Operation Cloud Hopper [4] attacks. In October 2020, sanctions were adopted in relation to the 2015 cyber-attack on the German Federal Parliament [5].

In June 2024, additional sanctions were adopted in response to cyber-attacks targeting critical infrastructure and government emergency response teams in the EU and Ukraine [6]. In January 2025, another package of sanctions was imposed in response to cyber-attacks against Estonia in 2020 [7].

More recently, in March 2026, the Council adopted additional restrictive measures targeting individuals and entities involved in cyber-attacks against the EU and its member states, further demonstrating the continued use of the framework [8].

Despite these developments, the practical use of the cyber sanction's framework remains limited when compared to the increasing frequency, complexity, and impact of cyber operations affecting the EU. This creates a tension between the formal availability of the instrument and its observable application in practice.

This raises a critical question as to whether the framework can be effectively applied using publicly available information. This issue concerns operational usability rather than political intent.

Cyber operations have evolved significantly since 2019. Many attacks are indirect, persistent, and difficult to attribute, challenging traditional assumptions regarding scale, impact, and responsibility.

Against this backdrop, this study examines the EU cyber sanctions framework as an operational instrument. It assesses whether the framework's criteria can be translated into usable indicators for analysing contemporary cyber incidents. It also examines to what extent these criteria can be applied using publicly available information.

In doing so, the research links legal design with empirical cyber-attack analysis.

Motivation of the study

Despite the existence of the EU cyber sanctions framework, limited academic attention has been given to its practical application as a policy instrument. Most existing studies

focus on sanctions effectiveness, as well as the political, legal, or strategic dimensions of sanctions.

Limited attention has been given to examining whether the cyber sanctions framework can be operationalised using publicly available information on cyber-attacks. This gap is significant, as the framework relies on criteria that require assessing the scale, impact, and significance under conditions of inherent uncertainty.

An operational perspective therefore allows for the evaluation of how these criteria function in practice, rather than how they are defined in theory.

The motivation for this study lies in the need to assess the usability of the EU cyber sanctions framework as an analytical and policy instrument in practice, particularly in view of the gap between legal criteria and observable evidence.

1.1 Research purpose

The purpose of this study is to examine the EU cyber sanctions framework as an operational policy instrument.

It assesses whether the framework's criteria for cyber-attacks with a significant effect can be translated into usable indicators using publicly available information. The study evaluates how selected cyber-attacks map against the framework's criteria and where practical challenges arise in their application.

This thesis examines the framework's usability and suitability for contemporary cyber operations. The research also identifies specific areas where clarification or refinement of the Regulation's criteria could improve operational applicability.

1.2 Research questions

RQ1: To what extent can the EU cyber sanctions framework's criteria be operationalised using publicly available information on cyber-attacks?

RQ2: How do selected cyber-attacks affecting the EU since 2019 map against the framework's criteria for identifying an attack with significant effect?

RQ3: Which criteria within the EU cyber sanctions framework present the greatest practical challenges when applied to contemporary cyber operations?

RQ4: What limited clarifications or adjustments to the framework's criteria could improve their operational applicability?

1.3 Scope, assumptions, and limitations

The scope of this thesis covers the EU's cyber sanctions framework as established by the Council from its adoption on 17 May 2019 onwards.

This study focuses on the framework's criteria for identifying cyber-attacks with a significant effect, as defined in Regulation (EU) 2019/796. Furthermore, this paper is limited to cyber-attacks constituting an external threat to the Union or its member states, as defined in the Regulation.

The analysis examines selected cyber-attacks affecting the EU or its member states since 17 May 2019 until 17 May 2025, based exclusively on publicly available information. The specific cyber-attacks are used as case studies selected to stress test the operational applicability of the framework's criteria and are identified in the methodology section.

This research does not assess the political decision-making, the attribution discourse, or confidential information underlying sanctions decisions.

The goal of this paper is to evaluate whether the EU cyber sanctions framework can be practically applied to contemporary cyber operations. A secondary objective is to identify targeted areas where clarification or refinement of the framework's criteria could improve operational usability.

1.3.1 Key assumptions

The author highlights the following key assumptions:

- The EU cyber sanctions framework is intended to be applied using information available to EU institutions and member states at the time of the assessment. This assumption is based on the operational nature of the framework under the CFSP

where decisions are taken on the basis of available evidence and situational awareness [3].

- Publicly available information provides a partial but meaningful basis for analysing the framework's criteria in relation to cyber-attacks. This assumption is supported by cybersecurity reporting practices and open-source intelligence, including the European Union Agency for Cyber Security (ENISA) and Computer Emergency Response Team for the EU (CERT-EU) reports.
- The framework's criteria are designed to function independently of formal attribution to a State or individual. This assumption is derived from Decision (CFSP) 2019/797 which states that the application of restrictive measures does not amount to attribution of responsibility to a State [3].
- Operational challenges may arise from the nature of cyber operations rather than from institutional reluctance or political intent. This assumption underpins the analytical focus of the study on structural and evidentiary constraints rather than political decision-making.
- The study does not assume that sanctions should have been imposed in any specific case. This assumption reflects the scope of the research, which focuses on operational applicability rather than policy or normative evaluation.

1.3.2 Limitations

The author highlights the following limitations:

- This research relies exclusively on open-source information. Classified or confidential information available to EU institutions and member states is out of scope. This limitation reflects the methodological choice of using publicly available data.
- Public reporting on cyber-attacks may be incomplete, inconsistent, or retrospective, which may limit the precision of impact assessment. This limitation reflects the evolving and often fragmented nature of cyber incident reporting.
- Economic loss to targets of cyber-attacks or economic benefit to perpetrators are not consistently quantifiable using publicly available information. This limitation is supported by the findings of this study and reflects broader challenges in measuring the financial impact of cyber-attacks.

- The selection of cyber-attacks used as case studies is limited in number. It is intended to support analytical stress testing rather than a fully-fledged assessment of all cyber-attacks affecting the EU and beyond. This limitation reflects the scope and design of the study.

2 Literature review

Sanctions have been included in the EU's diplomatic toolkit for decades.

Actors may impose sanctions not only to influence state and non-state actors, but also to promote foreign policy preferences and normative objectives [9]. Sanctions may therefore pursue multiple objectives, including signalling disapproval, constraining undesirable behaviour, and supporting broader foreign policy aims.

In the literature, sanctions are commonly understood as politically motivated penalties imposed after a target fails to observe international standards or obligations [9]. They are not limited to coercion. Sanctions may also constrain capabilities and signal disapproval to domestic and international audiences.

The evolution of targeted or "smart sanctions" reflects efforts to minimise collateral damage while maintaining political leverage [10]. Instruments such as asset freezes and travel bans, which form the core of the EU cyber sanctions regime, are key examples of such targeted measures.

This literature review establishes a conceptual baseline for analysing the EU cyber sanctions framework as a policy instrument. It examines how sanctions are conceptualised in the literature, how signalling and deterrence are discussed in cyber-related debates, and how CFSP decision-making conditions shape the use of cyber sanctions.

Beyond assessing effectiveness, the review focuses on a less explored dimension, namely the operational usability of sanctions frameworks. In particular, it considers whether abstract legal criteria can be translated into observable and applicable indicators in the context of cyber-attacks.

The review therefore identifies conceptual and institutional gaps relevant to assessing the practical application of the EU cyber sanctions framework since its establishment in 2019.

2.1 Sanctions effectiveness, signalling, and cyber deterrence

Scholarly work on sanctions has long focused on the question of effectiveness. Nevertheless, defining and measuring sanctions success and failure remains contested.

Sanctions regimes differ across actors, contexts, and instruments, which further complicates generalisation. Sanctioning measures such as asset freezes, travel bans, and embargoes are imposed across varying time periods and policy domains, making consistent evaluation difficult.

Early scholarly work on sanctions effectiveness, such as Pape [12], defines success in terms of total compliance by the targets.

Subsequent research adopts a broader perspective, suggesting that sanctions may still be considered effective even when they contribute partially to policy objectives or support negotiated outcomes [13], [14], [15], [16]. This interpretation represents a shift from binary success-failure assessments.

The literature further identifies a range of factors influencing sanctions outcomes.

These include the level of costs imposed on targets [17], [18], [19], whether sanctions are imposed unilaterally or multilaterally [19], [20], [21], and whether sanctions are designed to minimise collateral damage while targeting responsible actors [19], [10], [22]. These variables highlight the complexity of assessing sanctions across different contexts.

Giumelli argues that much of the effectiveness debate relies on a "*pain-gain*" logic [11]. This logic evaluates whether targets modify behaviour in response to imposed costs. However, this perspective does not fully explain why sanctions are used in situations where behavioural change does not to occur [11].

Compliance is therefore only one dimension of a broader political dynamic. It is not its defining outcome. In this context, sanctions are understood as instruments that serve multiple functions. Beyond coercion, they may constrain actors, signal disapproval, and reinforce normative commitments [11], [23].

Targeted sanctions, such as asset freezes and travel bans, exemplify this evolution by seeking to minimise collateral damage while maintaining political leverage.

Criticism often arises when assessing whether such measures “work”. Travel bans and asset freezes may inconvenience targets without producing substantial behavioural change. This broader understanding is relevant in the cyber domain, where observable behavioural change may be difficult to measure, and attribution may be contested.

As a result, sanctions may operate less as a tool of direct coercion and more as an instrument of signalling, deterrence, and norm reinforcement.

For this thesis, sanctions effectiveness is not assessed in terms of behavioural outcome. Instead, the literature is used to clarify the multiple logics through which sanctions operate. This provides a conceptual foundation for examining whether the legal criteria of the EU cyber sanctions framework can be operationalised in practice.

Building on this understanding, cyber sanctions may indicate disapproval, constrain actors, and demonstrate resolve. This is particularly relevant in the cyber domain, where attribution challenges, operational ambiguity, and the covert nature of cyber operations complicate direct responses. These characteristics also make observable outcome difficult to measure.

Deterrence in cyberspace is often conceptualised as the combination of credible consequences and communicated resolve. However, deterrence effects are difficult to verify empirically. Malicious cyber activities may remain undisclosed, attribution may be contested, and decision-making may rely on classified information. These factors limit the observability of deterrence outcomes.

Cyber sanctions can therefore be understood as part of a broader diplomatic toolkit. They may signal collective condemnation, increase costs for responsible actors, and reinforce norms of responsible behaviour.

This understanding aligns with arguments that sanctions serve multiple functions and must be assessed within their broader foreign policy context [11], [23]. However, signalling and deterrence logics do not resolve the practical challenge of applying legal thresholds to concrete cyber-attacks.

The opacity of cyber operations complicates not only deterrence assessment but also the practical evaluation of legal thresholds such as scale, impact, and significance.

While the literature discusses deterrence and signalling at a conceptual level, it provides limited methodological guidance. It does not explain how legal thresholds embedded in the EU cyber sanctions framework can be translated into observable indicators using publicly available information.

This gap is central to assessing operational usability. It also motivates the analytical focus of this study.

2.2 EU Common Foreign and Security Policy constraints and attribution politics

Within the EU context, sanctions have been analysed through the lenses of multilateralism, institutional decision-making conditions, and foreign policy coordination [11], [24], [25], [26], [27].

One recurring issue is the absence of a single agreed framework to assess sanctions success. Giumelli [9] identifies this lack of a common framework as a core challenge. Baldwin [28] similarly notes limited consensus in defining and measuring sanctions success.

Decision-making under the CFSP is central to understanding the use of EU sanctions. Article 29 of the Treaty on European Union authorises the Council to adopt sanctions by unanimity [29].

Financial measures, including asset freezes, are implemented under Article 215 of the Treaty on the Functioning of the European Union through qualified majority voting [30].

This structure demands political consensus and coordination among EU member states and institutions. It embeds sanctions decisions within collective political bargaining.

Sanctions under the CFSP are embedded in a highly political environment. Member states retain sovereignty in foreign policy and may differ in their threat perceptions, diplomatic priorities, and strategic interests. Such divergences may influence the willingness to adopt sanctions in cyber contexts.

These constraints become particularly relevant in cases involving contested attribution or sensitive intelligence assessments.

Decisions to impose cyber sanctions may rely on classified information that is not publicly disclosed. This creates asymmetry between the internal evidentiary basis for political decisions and the evidence available to external observers, including researchers and analysts.

Attribution in the cyber domain is both technical and political. While technical indicators may suggest responsibility, formal attribution remains a sovereign political act by EU member states. Public attribution statements may therefore reflect strategic considerations rather than full evidentiary disclosure, reinforcing the gap between evidence and publicly observable justification.

The EU adopted Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2][3]. The Regulation defines the scope of covered cyber-attacks and establishes that sanctions may apply to attacks with a "*significant effect*" constituting an external threat to the Union or its member states [2].

Article 2 of the Regulation sets out the factors determining whether a cyber-attack produces a *significant effect*.

Cyber sanctions consist primarily of travel bans and asset freezes against natural or legal persons involved in such attacks. Listing individuals does not constitute formal attribution to a third state [2].

This separation allows political flexibility. However, it may also limit transparency regarding the evidentiary basis of sanctions listings.

Scholars have examined the EU cyber sanctions regime from institutional and operational perspectives.

Kozłowski [31] has analysed obstacles related to attribution, member state coordination, and evidentiary communication in the context of EU cyber responses. At the time of this study, the EU cyber sanctions regulatory framework has not yet been fully operationalised.

Miadzvetskaya [32] has examined challenges concerning legal and technical attribution, divergences among member states, evidentiary standards, and fundamental rights considerations under the CFSP.

Kapsokoli [33] has analysed technical, political, and judicial parameters influencing the imposition of cyber sanctions, including attribution complexities and normative frameworks governing responsible state behaviour.

These studies identify institutional, political, and evidentiary challenges surrounding the EU cyber sanctions regime. However, they do not systematically examine how the framework's legal thresholds operate when confronted with concrete cyber-attacks documented through publicly available sources.

This leaves a gap between legal design and empirical application. This unresolved question provides the foundation for the present study.

2.3 Operational and evidentiary challenges in applying cyber sanctions

Operational and evidentiary challenges arise directly from the structure of Regulation (EU) 2019/796.

Article 1 defines the scope of cyber-attacks covered by the framework and specifies when such attacks constitute an external threat to the Union or its member states.

Article 2 sets out the factors determining whether a cyber-attack produces a "*significant effect"*. These factors include scope, scale, severity of disruption, number of affected persons or member states, economic loss, economic benefit to perpetrators, and the nature or scale of accessed data [2].

Although these criteria are explicitly enumerated, the Regulation does not establish quantitative thresholds, weighting mechanisms, or methodological standards for their application.

For example, the reference to "*economic loss*" does not clarify whether such loss must reach a specific monetary level, how it should be calculated, or whether it must be directly attributable to the cyber operation.

Similarly, the reference to the "*number of persons affected*" does not specify whether this criterion must reach a particular scale, or whether it operates cumulatively with other criteria.

The criterion concerning the "*number of member states affected*" also raises interpretative questions. The Regulation does not operationalise the role of cross-border impact in determining a significant effect. Although practice indicates that a severe impact within a single member state may suffice, the absence of explicit guidance introduces ambiguity. It also limits consistency in the application of this criterion.

In addition, several criteria rely on qualitative assessment.

Disruption of "*critical state functions*" or interference with "*essential services*" requires contextual interpretation. While the Regulation identifies relevant sectors, it does not define operational indicators for determining when disruption becomes legally significant, leaving substantial interpretative discretion.

Article 2 establishes the legal basis for listing natural or legal persons responsible for, involved in, or associated with cyber-attacks that meet the criteria set out in Article 1. Article 2 does not redefine the elements of *significant effect*. Instead, it enables the EU to adopt sanctions once the conditions under Article 1 are fulfilled.

In practice, imposed cyber sanctions are accompanied by statements of reasons published by the EU. These statements summarise the conduct attributed to listed persons but do not disclose the full evidentiary reasoning underlying the assessment, limiting external verification of how the criteria are applied.

This institutional structure means that the applicability of Articles 1 and 2 of Regulation (EU) 2019/796 operates within political and evidentiary constraints. The legal criteria are formulated in generic terms, while publicly available reporting on cyber-attacks varies significantly in depth, precision, and methodological transparency.

The methodological challenge examined in this thesis therefore arises from the interaction between broadly framed legal standards and heterogeneous public evidence. It does not arise from assumptions introduced by the author.

This grounds the study in structural constraints rather than subjective interpretation.

2.4 Novelty

This study contributes to existing literature by examining the EU cyber sanctions framework from an operational perspective.

Existing literature has analysed cyber sanctions effectiveness, institutional decision-making under the CFSP, and the strategic logic of cyber responses. These studies primarily focus on political objectives, legal design, or strategic signalling.

Nevertheless, limited attention has been given to the practical application of the framework's legal thresholds to concrete cyber-attacks.

This thesis therefore shifts the focus from evaluating political outcomes to assessing whether the framework's criteria can be translated into observable and workable indicators, using publicly available information.

By examining how selected cyber-attacks interact with the Regulation's thresholds, the study identifies evidentiary ambiguities, measurement challenges, and operational constraints.

This research bridges legal design and empirical cyber-attack analysis. It offers a structured approach to assessing operational usability without evaluating political intent or relying on classified evidence.

3 Research methods

This research uses qualitative document analysis combined with an incident-based stress testing approach to assess the operational applicability of the EU cyber sanctions framework.

Document analysis is a recognised qualitative research method for evaluating and interpreting policy frameworks and institutional practices through written, visual, or digital material [34]. This method is suitable for this study because information on the EU cyber sanctions framework and cyber-attacks is mainly available through official documents and open-source reporting.

While stress testing was originally developed to analyse the resilience of financial institutions, the core principles of this approach are adapted in this study.

According to the Basel Committee on Banking Supervision, stress testing is a risk management practice designed to assess resilience under adverse scenarios [35]. Similarly, stress testing is widely used in European regulatory practice to analyse institutional resilience across the banking and non-financial systems [36].

In this paper, stress testing is understood as a systematic comparison of the EU cyber sanctions framework's criteria against observable characteristics of cyber-attacks.

Unlike financial stress testing, which relies on quantitative modelling, this study applies a qualitative stress testing logic. It does so by challenging each legal criterion against documented cyber-attack characteristics.

Drawing on this risk-based logic, this approach assesses how the framework performs when tested with cyber-attacks that may challenge its thresholds and scope. The stress test is qualitative and exploratory in nature. It focuses on alignment and gaps between regulatory criteria and documented cyber-attack evidence, rather than statistical measurement.

3.1 Research design

The research relies exclusively on secondary data gathered from publicly available and verifiable sources. The dataset includes EU legal instruments, analytical and media reporting on cyber-attacks, and relevant academic and policy literature.

Content analysis is used to screen documents for relevance in line with the research questions [34]. It is also used to extract information relevant to the framework's operational criteria.

Thematic analysis supports the identification of recurring patterns related to the characteristics of cyber-attacks, observable impacts, and potential implementation gaps within the framework [34].

The findings are interpreted by examining how selected cyber-attacks interact with the framework's criteria. This helps identify strengths, limitations, and areas of potential misalignment.

This research design allows the EU cyber sanctions framework to be treated as the object of study. Cyber-attacks serve as empirical stress tests.

The unit of analysis is the interaction between legal criteria and documented cyber-attack characteristics. It is not the political motivations of perpetrators or the effectiveness of sanctions outcomes.

3.2 Data sources

Legal and policy documents forming the EU cyber sanctions framework are referenced in this study. These include Regulation (EU) 2019/796, which is legally binding and directly applicable in all EU member states. Decision (CFSP) 2019/797 is also referenced where relevant, as it governs the political implementation of cyber sanctions.

To identify cyber-attacks relevant to this study, the open-access database of the European Repository of Cyber Incidents (EuRepoC) was used [37].

This database is a project of the German Institute for International and Security Affairs. It is funded by the German Foreign Office and the Danish Ministry of Foreign Affairs. The EuRepoC project team includes researchers from Austria, Estonia, and Germany.

The repository includes information on over 4,200 politically relevant cyber incidents[6] from January 2000 to the present and updated daily [37].

The political dimension of cyber incidents is relevant because sanctions are, by definition, a political instrument. However, this thesis does not assess the political motivation or intent behind cyber-attacks.

Instead, it examines whether selected cyber-attacks meet the legal conditions set out in Article 1 of Regulation (EU) 2019/796. It also examines whether they would plausibly justify listings under Article 2 based on observable evidence.

Political relevance assists in identifying cases of CFSP interest but does not determine sanctions applicability. A politically relevant cyber-attack may still fail to meet the Regulation's thresholds due to limited observable impact.

The core question is whether the selected cyber-attacks satisfy the Regulation's scope conditions under Article 1. It also considers whether they meet the "*significant effect"* factors listed in Article 2, based on publicly available information.

Public reporting sources include official statements by EU member states and relevant institutions, technical reports, and reputable media reporting.

Classified or confidential information is outside the scope of this thesis.

3.3 Case study selection criteria

Cyber-attacks selected for the case studies are identified based on legal conditions set out in Articles 1 and 2 of Regulation (EU) 2019/796.

[6] From the German Institute for International and Security Affairs: "This includes incidents that have not yet been politicised and cases where no political motivation and/or affiliation of the attacker(s) has been reported"

Article 1 defines the scope of covered cyber-attacks and the requirement that they constitute an external threat.

Article 2 sets out the factors determining whether such attacks produce a *significant effect.*

The selection criteria therefore reflect both the scope conditions under Article 1 and the significant effect factors listed in Article 2.

These factors are assessed qualitatively using observable indicators rather than precise quantification.

For the purpose of this study, the selected cyber-attacks must have occurred between 17 May 2019 and 17 May 2025.

The selection criteria are as follows:

- Cyber-attacks must involve unauthorised access to information systems, information system interference, data interference, or data interception;
- Cyber-attacks must have affected the EU or at least one EU member state;
- Cyber-attacks must plausibly constitute an external threat within the meaning of the Regulation;
- Cyber-attacks must be documented in reliable publicly available sources, including official statements, technical reports, or reputable media reporting;
- Cyber-attacks must present observable impacts relevant to the framework's criteria for identifying a *significant effect*;
- Attempted cyber-attacks may be included if potential impact is documented;
- Cyber-attacks must not have resulted in the imposition of EU cyber sanctions;
- Cyber-attacks are selected to reflect different types of cyber operations, including data compromise, disruption, or long-term intrusion.

Case study selection is guided by the criteria set out in Article 1 of Regulation (EU) 2019/796, while the assessment relies exclusively on publicly available information.

Article 1 defines cyber-attacks constituting an external threat as those that originate from outside the Union. It also includes attacks that use infrastructure located outside the Union or are conducted with the support or direction of such actors.

The verification of these elements requires attribution concerning the origin of the attack, the infrastructure used, or the identity and location of the actors involved. However, as reflected in Council Decision (CFSP) 2019/797, attribution of responsibility for cyber-attacks is a sovereign political decision. It is taken by EU member states on a case-by-case basis and is distinct from the imposition of cyber sanctions [3].

As a result, the external threat criterion cannot always be conclusively established on the basis of publicly available information.

Instead, cyber-attacks are selected where available reporting, technical analysis, and their classification in the EuRepoC database indicate that they plausibly fall within the scope of Article 1.

This approach reflects an operational constraint inherent in open-source analysis, rather than a limitation specific to individual case studies.

3.3.1 Application of the case study selection criteria

The EuRepoC dashboard was used to filter cyber incidents affecting EU member states within the defined timeframe.

Geographic filtering was applied individually for each EU member state. Incidents were filtered to display records from 17 May 2019 to 17 May 2025.

Initial screening was based on Article 1 of Regulation (EU) 2019/796, which defines the scope of cyber-attacks constituting an external threat. This includes threats to the EU or its member states.

EuRepoC relies on publicly available information, including open-source attribution indicators. While attribution information provides a plausible screening threshold, it does not provide legal certainty.

Records were screened by reviewing incident titles, descriptions, documented impacts, attribution indicators, and linked sources. Variation in targets and attack types was ensured. Incidents affecting critical infrastructure or State functions were prioritised.

Incidents were excluded where one or more selection criteria were not met. Incidents with minimal or negligible observable impact were also excluded.

Shortlisted incidents were transposed into an Excel database for further structured screening. Additional publicly available sources were reviewed to complement details on affected sector, perpetrators, relevance to Article 1 scope, and relevance to Article 2 *significant effect* factors.

3.3.2 Shortlisted cyber incidents

The screening resulted in a final list of ten cyber incidents meeting the selection criteria. An overview is presented in Appendix 2 – Shortlisted cyber-attacks.

Three cyber incidents were selected for in-depth stress testing. This number allows a systematic mapping of each incident against the Regulation's criteria using a consistent indicator framework.

The selection strategy follows a most-likely logic. Incidents were chosen because they plausibly challenge the Regulation's thresholds due to scale, sectoral impact, or cross-border relevance.

This allows the framework to be tested under demanding conditions.

3.4 Stress testing and operationalisation

The analysis maps observable characteristics of cyber-attacks against the factors listed in Article 2 of Regulation (EU) 2019/796.

Each Article 2 factor is operationalised through qualitative indicators derived from publicly available reporting.

For example, economic loss is assessed through documented financial damage estimates. Sectoral disruption is assessed through reports of service interruption. Cross-border relevance is assessed through documented geographic impact.

The operationalisation does not assign numerical scores. Instead, it evaluates whether available evidence plausibly satisfies each Article 2 factor.

The same indicator framework is applied consistently across all case studies to ensure comparability and transparency.

The assessment is qualitative in nature, but rule based. It remains anchored in the legal wording of Articles 1 and 2 and applies consistent interpretative standards across cases.

3.5 Validation and limitations

The reliance on publicly available information may result in incomplete evidentiary mapping. This is because intelligence assessments and classified information underlying EU decision-making are not accessible to the researcher.

Open-source reporting may vary in depth, reliability, and methodological transparency. To mitigate this limitation, multiple sources are reviewed where possible, and conclusions are based on verifiable data only.

This research relies exclusively on open-source information. While efforts were made to consult official reports, institutional publications, technical analysis, and reputable media coverage, public information ecosystems are dynamic and continuously evolving. It is therefore possible that additional information exists beyond the sources consulted.

Nevertheless, the objective of this study is not to reconstruct a complete factual record of each cyber-attack. Instead, it assesses whether sufficiently documented evidence exists to operationalise Article 2 criteria.

The structured source selection process and consistent application of inclusion criteria mitigate the risk of arbitrary or selective evidence use.

Finally, the study does not assess the internal political deliberations of EU institutions and member states. It also does not claim to replicate the evidentiary standard applied by the Council.

The most significant limitation of this study is its exclusive reliance on publicly available information. This approach restricts the ability to assess attribution, evidentiary thresholds, and economic impact. It cannot provide the same level of detail available to EU member states and institutions. As a result, certain conclusions remain contingent on incomplete or evolving information. Future research could address this limitation through expert interviews, confidential institutional data, or detailed case studies conducted in cooperation with relevant authorities.

3.6 Ethical considerations

Ethical considerations arise in relation to the author's interpretation and data handling. To minimise bias, the analysis follows predefined legal criteria and applies consistent indicators across case studies.

No classified or confidential information is used. The research relies exclusively on publicly documented cyber-attacks and institutional sources. No personal data beyond publicly reported information is processed.

4 Case studies: Incident-based stress testing

In this study, incident-based stress testing is used to assess the operational applicability of the EU cyber sanctions framework.

This approach draws on key principles of traditional stress testing. These include performance under adverse conditions, examining resilience against predefined criteria, and identifying structural weaknesses in demanding scenarios.

Incident-based stress testing in this study serves to systematically compare the EU cyber sanctions framework's criteria against observable characteristics of selected cyber-attacks. The selected cyber-attacks are analysed as case studies.

The approach is qualitative in nature. It assesses each legal criterion under Article 2 of Regulation (EU) 2019/796 against documented cyber-attacks affecting the Union or its member states.

In doing so, this chapter addresses the following research questions:

- RQ1: To what extent can the EU cyber sanctions framework's criteria be operationalised using publicly available information on cyber-attacks?
- RQ2: How do selected cyber-attacks affecting the EU since 2019 map against the framework's criteria for identifying an attack with significant effect?

The stress-testing exercise evaluates how the framework performs when confronted with cyber-attacks that plausibly challenge its legal thresholds. This exploratory assessment enables the identification of alignment or gaps between the Regulation's legal criteria and publicly documented evidence on cyber-attacks.

The case studies are organised into three main sections. The first section outlines the characteristics of the cyber-attack, including a timeline of events, its impact, and the aftermath. The second section maps the observable characteristics of the cyber-attack against Article 2 of Regulation (EU) 2019/796. The final section identifies operational challenges arising from this mapping exercise.

Three case studies are conducted to allow for a structured cross-case comparison. The case studies are limited to the selection criteria derived from Article 1 and preliminary screening against Article 2 of Regulation (EU) 2019/796.

Selected cyber-attacks must also have occurred between 17 May 2019 and 17 May 2025. The data used consists exclusively of open-source information available at the time of writing.

This chapter does not evaluate the political intent of cyber operations. The purpose is not to assess whether the EU should impose sanctions, but to examine whether the framework's legal criteria are operationally applicable to contemporary cyber operations.

4.1 Case study: Ransomware attack targeting the Health Service Executive

This case study examines a ransomware attack that affected the Health Service Executive (HSE) of Ireland in 2021. It was selected because it plausibly challenges the thresholds of Regulation (EU) 2019/796.

The following sections first outline the factual characteristics of the attack and its aftermath. They then qualitatively assess whether these characteristics plausibly satisfy the Article 2 criteria of the Regulation. The final subsection highlights the operational and evidentiary challenges identified through this incident-based stress test.

4.1.1 Incident overview and impact

The HSE is a large organisation responsible for delivering public health and social care services across Ireland.

According to a December 2021 report from PricewaterhouseCoopers (PwC), the HSE operated approximately 4,000 locations, including 54 acute care hospitals [38]. It also employed over 130,000 staff, making it the largest employer in Ireland at the time [38].

The HSE is classified as an Operator of Essential Services under the EU Network and Information Security Directive, reflecting its status as critical infrastructure [38].

The ransomware attack originated from a phishing email opened on 16 March 2021. This led to a malware infection on a HSE workstation on 18 March 2021 [*ibid*].

Following initial access, the attacker operated within the HSE's IT environment for approximately eight weeks. Conti ransomware was deployed on 14 May 2021 [*ibid*]. During this period, the attacker performed lateral movement across the network and compromised multiple systems.

Upon detection on 14 May 2021, the HSE disconnected its national healthcare network from the internet. It also shut down IT systems in an attempt to contain the attack. This response aimed to prevent the further spread of the ransomware.

However, it resulted in nationwide loss of access to clinical and non-clinical systems. Those systems included patient information systems, laboratory systems, imaging systems, payroll, internal email infrastructure, and procurement services [*ibid*].

The attackers demanded a ransom of approximately $20 million in exchange for the decryption key [39]. The HSE decided not to pay the ransom.

The technical impact on the HSE was extensive. According to the incident response investigation, approximately 80% of the IT environment was affected by encryption [38]. Over 2,800 servers and 3,500 workstations across multiple domains showed evidence of encryption [38].

The scale of disruption required a phased recovery process. Although certain core systems were recovered within days, the wider decryption and rebuilding of servers and applications extended over several months.

A significant development occurred on 20 May 2021, when the attackers released a decryption key to the HSE for free. However, the malicious actors warned the HSE they would publish or sell private data if the ransom was not paid [40], [41].

The decryption tool was validated and adapted by external cybersecurity specialists. This enabled the restoration of encrypted systems. Without the release of the decryption key, recovery would likely have taken considerably longer and may have resulted in more substantial data loss [38].

The ransomware attack had significant operational consequences across the Irish public healthcare system.

Healthcare professionals reverted to manual processes, these included handwritten laboratory requests and paper-based patient record management [38]. Radiotherapy services and non-emergency radiation treatments were suspended at multiple centres, while diagnostic services were cancelled or postponed. Elective inpatient procedures and outpatient clinics were disrupted nationwide [42].

These system-wide disruptions raised concerns regarding patient safety and continuity of care.

In addition to system encryption, the attack involved illegal access to and copying of data from the HSE's IT environment.

Following forensic analysis of the breach, it was anticipated that the HSE would notify 113,000 individuals. Their personal data had been illegally accessed and copied, as confirmed in a parliamentary response by the Irish Minister for Health [45].

According to the HSE, the compromised data consisted of personal, financial, and medical information, as well as internal health services files [43], [44].

A limited sample of stolen data was published online by the attackers in May 2021 as an attempt to extort the HSE. The HSE subsequently obtained a High Court injunction prohibiting the sharing or sale of the compromised data [38], [39].

This cyber-attack raised significant data protection concerns. It also led to engagement with the Irish Data Protection Commission under the General Data Protection Regulation (GDPR).

The notification process and subsequent investigations illustrate the complexity of assessing the full scope of data breaches. This is especially difficult after a cyber-attack affecting critical infrastructure.

Non-clinical impacts were also considerable. Delays occurred in administrative processes, including public service procedures reliant on the HSE email systems and certain payroll-related payments.

Staff experienced operational strain during the prolonged recovery period. Significant resources were required to manually re-enter and reconcile clinical information into restored systems.

By 21 September 2021, approximately 130 days after the ransomware detonation, 99% of applications had been restored and 100% of the servers were decrypted [38].

From a financial perspective, the PwC report does not quantify a consolidated total economic loss figure. However, it documents substantial direct expenditure associated with the incident and remediation efforts [38].

Recovery, cybersecurity enhancements, and resilience improvements required significant additional investment. Long-term cybersecurity transformation costs were also projected to extend over several years [38].

The absence of a quantified loss figure reflects the complexity of assessing economic damage arising from large-scale cyber-attacks affecting public healthcare systems.

In the years following the attack, the repercussions extended beyond technical recovery.

By 2024, the HSE faced multiple lawsuits alleging damages linked to data exfiltration and operational disruption caused by the 2021 incident. Legal filings reportedly numbered in the hundreds, reflecting broader societal and personal costs attributed to the breach.

In February 2026, the Cork Circuit Court was scheduled to hear motions from individuals alleging harm from the cyber-attack. These motions related to victims' civil claims against the HSE [50].

This ongoing litigation highlights the long-lasting societal and legal repercussions of the incident. These include claims for personal loss, sensitive data exposure, and associated harm.

The 2021 attack has been attributed in open-source reporting to the Conti ransomware group. This group is often associated with the organised cybercrime network known as "Wizard Spider"[7].

Conti ransomware was considered a highly disruptive human-operated ransomware variant at the time. It involved data exfiltration and network-wide encryption.

In subsequent years, members associated with organised ransomware networks were targeted with sanctions by the United Kingdom and the United States [52]. This included actors linked to Conti and reflected the transnational character of such groups [52].

Taken together, the scale, duration, sectoral sensitivity, financial implications, and legal consequences of the 2021 cyber-attack show why this case plausibly challenges multiple thresholds under Regulation (EU) 2019/796.

4.1.2 Mapping to legal criteria

In this section, the observable characteristics of the cyber-attack are mapped to Article 2 of Regulation (EU) 2019/796 through qualitative indicators.

The analysis does not assign numeric scores. Instead, it evaluates whether publicly available evidence plausibly satisfies each Article 2 factor.

For the purpose of this study, a factor is considered to be **plausibly satisfied** where open-source evidence provides sufficient factual support. The evidence must reasonably align the cyber-attack characteristics with the wording of the relevant Article 2 criterion.

A factor is considered **partially satisfied** where some relevant evidence exists, but ambiguity remains due to lack of quantification, incomplete information, or interpretative uncertainty.

A factor is considered **not satisfied** where publicly available evidence does not support alignment with the criteria.

[7] According to publicly available information from the United Kingdom's Government, key group members allegedly maintained links to Russian Intelligence Services.

The qualitative indicators used in this assessment are derived directly from the legal wording of Article 2.

For example, indicators relating to “scope and severity” include duration of disruption, extent of service disruption, and institutional impact. Indicators relating to “economic loss” include documented reported damages or financial expenditure. Indicators relating to “data stolen” include confirmed data exfiltration or exposure of sensitive information.

Since the Regulation does not establish weighting mechanisms or numerical thresholds, the assessment remains interpretative, but rule based.

The absence of publicly available evidence is treated as an evidentiary limitation rather than proof that a criterion is not met. The same interpretative framework is applied consistently across all case studies to ensure comparability.

4.1.2.1 Article 2(a): scope, scale, impact or severity of disruption

Article 2(a) requires an assessment of the scope, scale, impact, or severity of disruption caused, including effects on essential services, critical State functions, public order or public safety.

Regarding the scope, the ransomware disruption affected Ireland’s public healthcare system, which operated approximately 4,000 locations and employed over 130,000 staff [38]. The attack resulted in the shutdown of core IT infrastructure across acute hospitals and administrative functions [*ibid*]. Therefore, the disruption was nationwide rather than localised.

Regarding scale and duration, approximately 80% of the HSE IT environment was encrypted, affecting over 2,800 servers and 3,500 workstations [*ibid*].

Full restoration of applications extended over 130 days [*ibid*]. This evidence indicates sustained impairment rather than short-term technical interruption.

Regarding impact and severity, the ransomware attack directly affected the delivery of essential healthcare services [38].

Hospitals reverted to manual processes. Several facilities also postponed or cancelled outpatient clinics, radiotherapy, and diagnostic imaging [38], [42].

The widespread cancellation of diagnostics and non-emergency treatments created risks to patient safety and the continuity of care. Therefore, the disruption extended beyond technical damage as it materially affected an essential public service.

Lastly, public healthcare is considered critical infrastructure and an essential service under EU law [38]. Accordingly, the impairment of the HSE system falls within the types of disruption under Article 2(a).

On the basis of publicly available evidence, Article 2(a) is plausibly satisfied.

4.1.2.2 Article 2(b): the number of natural or legal persons, entities or bodies affected

Article 2(b) requires the assessment of the number of persons, entities or bodies affected by the cyber-attack.

In the present case, the affected entity was Ireland's national public healthcare authority.

At the time, it operated approximately 4,000 locations and 54 acute hospitals across the State [38]. Therefore, the disruption extended beyond a single facility. It impaired nationwide institutional structure.

Regarding the number of affected persons, it was anticipated that approximately 113,000 individuals would be notified that their personal data had been illegally accessed and copied during the incident [45].

This figure includes both patients and HSE staff whose data was confirmed to have been compromised following forensic investigation [40], [45].

In addition to the data breach, the cyber-attack also caused disruption to healthcare services across Ireland, resulting in cancelled appointments, diagnostic delays, and temporary suspension of certain clinical services during the system outage.

It is essential to note that publicly available sources do not provide a consolidated figure for the total number of affected patients. This includes patients affected by postponed or cancelled appointments during the outage. The absence of a quantified total reflects an evidentiary limitation rather than an indication of limited impact.

Since the Regulation does not establish a quantitative threshold for the number of persons affected, the confirmed scale of the data breach and the nationwide institutional reach of the HSE indicate that a significant number of persons were impacted by the cyber-attack.

On the basis of publicly available evidence, Article 2(b) is plausibly satisfied.

4.1.2.3 Article 2(c): the number of member states concerned

Article 2(c) requires consideration of the number of EU member states directly concerned by the cyber-attack.

In the present case, the ransomware attack disrupted Ireland's national public healthcare system. There is no publicly available evidence that the same incident directly affected infrastructure or essential services in other EU member states.

The PwC post-incident report[8] outlines international law enforcement engagement and references similar incidents affecting healthcare institutions outside the EU. However, it does not demonstrate that additional EU member states were directly affected by this incident [38].

Based on the evidence available, the cyber-attack clearly concerns one member state, while cross-border effects on other EU member states are not documented.

On the basis of publicly available evidence, Article 2(c) is partially satisfied.

4.1.2.4 Article 2(d): the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property

Article 2(d) requires consideration of the amount of economic loss caused by the cyber-attack.

Public reporting indicates that the HSE estimated the immediate costs associated with the cyber-attack at approximately €102 million [50], [53], [54]. Publicly available reporting does not provide a detailed breakdown of this figure.

[8] See reference 37: PricewaterhouseCoopers (PwC), "Conti cyber attack on the HSE: Independent Post Incident Review"

Separately, the Comptroller and Auditor General[9] reported that in 2021 the HSE (excluding voluntary agencies) incurred €37 million in revenue expenditure and €14 million in capital expenditure directly associated with the cyber-attack [39].

According to the Comptroller and Auditor General, the reported costs associated with the cyber-attack were distributed across several categories:

- €17 million for professional services, including vendor support, investigation, remediation and security monitoring services;
- €13 million in incremental cyber-related costs incurred by HSE hospitals;
- €14 million in ICT hardware, including replacement of legacy devices and monitoring infrastructure;
- €7 million in other costs, including software acquisition and migration to Office 365 for a more secure cloud-based system [39].

In addition, revenue costs of approximately €4.4 million were expensed in 2022, primarily relating to Microsoft Office 365 [39].

The Comptroller and Auditor General further outlined that the full cost of the attack has not been comprehensively quantified. Costs incurred by voluntary agencies were not accounted for, and staff time associated with maintaining manual systems and subsequent data reconciliation was not costed [39].

Beyond immediate recovery costs, the HSE prepared an investment plan to implement recommendations arising from the PwC post-incident review.

Initial estimates indicated that almost €657 million would be required over a seven-year period. This amount related to cybersecurity improvements and resilience measures [39].

This projected expense reflects long-term remediation triggered by the incident. It does not represent direct financial damage at the time of attack.

[9] An independent constitutional officer responsible for public audit in Ireland.

In addition, the cyber-attack generated ongoing civil litigation. According to public reporting, approximately 620 legal proceedings had been initiated in connection with the data breach [50], [55].

It has been indicated that the HSE proposed compensation payments of €750 per affected individual, together with €650 toward legal costs [50], [55]. The total financial exposure arising from these proceedings remains uncertain.

While the legal proceedings may lead to additional financial liabilities, the total exposure from the lawsuits has not been quantified. Therefore, it cannot be included as a confirmed component of the economic loss caused by the cyber-attack.

Taken together, the documented audited expenditure, the broader immediate cost estimate, projected remediation investment, and ongoing legal liabilities demonstrate substantial economic consequences. They also show that the cyber-attack generated measurable financial effects.

On the basis of publicly available evidence, Article 2(d) is plausibly satisfied.

4.1.2.5 Article 2(e): the economic benefit gained by the perpetrator, for himself or for others

Articles 2(e) requires consideration of the economic benefit gained by the perpetrators as a result of the cyber-attack.

Public reporting indicates that the attackers demanded a ransom of approximately $20 million in exchange for the decryption key [39]. The HSE publicly confirmed that it did not pay the ransom [39].

On 20 May 2021, the attackers released a decryption key for free while continuing to threaten publication or sale of stolen data [40], [41].

While the ransom demand demonstrates a clear intent to obtain financial gain, there is no available evidence that the perpetrators received payment or realised measurable benefit from the cyber-attack.

Although ransomware groups commonly engage in data extortion or sale, this activity has not been conclusively documented in relation to the HSE attack.

On the basis of publicly available evidence, Article 2(e) is partially satisfied, as economic benefit was clearly sought but not evidently obtained.

4.1.2.6 Article 2(f): the amount or nature of data stolen or the scale of data breaches

Article 2(f) requires consideration of the nature and quantity of data stolen, accessed, or otherwise compromised during the cyber-attack.

The ransomware attack against the HSE involved unauthorised access to and copying of personal, financial, medical, and internal administrative data [43], [44].

Public reporting from the HSE indicates that the accessed personal data consisted of names, addresses, phone numbers, email addresses, Personal Public Service numbers, and employee numbers for HSE staff.

Financial data included bank account numbers, IBAN, and sort code. Medical data consisted of medical notes, treatment histories, and patient numbers.

Finally, internal administrative files consisted of forms submitted by staff members related to leave. They also included financial data concerning staff travel expenses [43], [44].

The exposure of sensitive personal and medical information significantly increases the potential societal and individual impact of the ransomware. Especially considering the sensitive nature of healthcare data and the scale of the affected healthcare infrastructure.

The cyber-attack involved confirmed data access to sensitive personal and medical data belonging to a large number of individuals.

On the basis of publicly available evidence, Article 2(f) is plausibly satisfied.

4.1.2.7 Article 2(g): the nature of commercially sensitive data accessed

Article 2(g) requires consideration of the nature of commercially sensitive data accessed during the cyber-attack.

Publicly available reporting indicates that the ransomware attack against the HSE involved unauthorised access to and copying personal, medical, financial, and internal administrative data [43], [44].

Internal administrative and financial information may also be considered commercially sensitive organisation data. This is particularly in the context of internal financial processes and public sector procurement.

Given the limited publicly available evidence regarding the extent of commercially sensitive data accessed, it is not possible to determine whether this criterion is fully satisfied.

On the basis of publicly available information, Article 2(g) is partially satisfied.

The outcome of mapping the HSE 2021 cyber-attack characteristics against Article 2 criteria of Regulation (EU) 2019/796 is illustrated in Table 2.

4.1.3 Operational challenges identified

The incident-based stress testing of the HSE 2021 cyber-attack highlights several operational challenges associated with applying the Article 2 legal criteria of Regulation (EU) 2019/796 to cyber-attacks using publicly available information.

Firstly, the analysis illustrates the absence of quantitative thresholds within the Regulation.

Several Article 2 factors rely on qualitative indicators such as scope, significant economic loss, or severity. However, the Regulation does not specify measurable benchmarks for these factors. As a result, the assessment requires interpretative judgment rather than predefined metrics.

Secondly, the case study outlines evidentiary limitations associated with publicly available information.

Open-source data provides substantial insights into the incident, including estimated costs, data breach notifications, and technical disruption. However, specific elements remain uncertain or incomplete.

For example, publicly available sources do not consolidate figures for the total number of patients affected by service disruptions. They do not provide the total number of cancelled medical appointments. In addition, the full scope of compromised data and its potential misuse remains partially undisclosed.

These limitations highlight the challenges of assessing cyber-attacks without access to investigative or confidential operational data.

Thirdly, the analysis highlights ambiguity in determining the number of affected persons or entities.

The HSE operates a complex nationwide healthcare system consisting of clinics, hospitals, and administrative services. Publicly available information confirms that approximately 113,000 individuals were expected to be notified in connection with the data breach. However, the total number of persons indirectly affected by the healthcare service disruptions remains uncertain [45].

Lastly, the case study reveals uncertainty in assessing the full economic loss of cyber-attacks. Although audited figures and public reporting provide substantial evidence of immediate and long-term costs, the overall economic impact remains difficult to quantify.

Following a post-incident analysis, PwC reported significant recovery expenses and long-term cybersecurity investments [38]. Furthermore, ongoing litigation expenditure related to the data breach introduces an additional dimension of potential financial liabilities.

The distinction between direct operational losses, long-term remediation investments, and indirect legal consequences requires interpretative judgement. This is relevant when applying Article 2(d).

In sum, these challenges highlight that the application of the EU cyber sanctions framework to cyber-attacks involves significant interpretative and evidentiary constraints. Although the legal criteria provide a structured framework, their operational use depends heavily on the availability and precision of public information.

4.2 Case study: Ransomware attack targeting Hospital Clínic de Barcelona

4.2.1 Incident overview and impact

The second case study examines a ransomware attack that affected the Hospital Clínic de Barcelona (HCB) in March 2023.

The HCB is one of the largest public hospitals in Spain and a major healthcare entity within the Catalan health system.

The cyber-attack also affected the information system shared with the Fundació de Recerca Clínic Barcelona-Institut D'investigacions Biomèdiques August Pi i Sunyer (FRCB-IDIBAPS). This institution conducts biomedical research associated with the hospital [56].

On 5 March 2023, the hospital's IT infrastructure was targeted by a ransomware attack. Open-source data attributes the attack to the RansomHouse ransomware group [57], [58], [59].

According to CERT-EU, the attack severely disrupted the hospital's information systems. It prevented access to several digital services necessary for clinical operations. HCB staff lost access to electronic medical records, pharmacy systems, radiology services, and laboratory systems. This forced healthcare professionals to rely on manual procedures and paper-based documentation. [60]

The cyber-attack affected not only the HCB but also organisations that shared parts of the same IT infrastructure.

Several research institutions and primary care centres connected to the HCB digital environment also experienced disruptions during the attack [60]. In addition, the cyber-attack impacted the information systems shared with FRCB-IDIBAPS [56].

According to CERT-EU, the attack involved a sophisticated intrusion targeting virtual environments within the HCB's infrastructure. The Catalonia authorities indicated that the attack did not rely on conventional intrusion techniques. They also stated that it demonstrated a degree of technical complexity, suggesting an evolution of methods used by the RansomHouse group. [60]

The operational impact of the ransomware on healthcare services was substantial. The disruption led hospital staff to postpone or temporarily suspend various medical procedures and outpatient consultations.

According to public reporting, approximately 300 surgical procedures were cancelled [57], [58], [61]. More than 11,000 outpatient consultations and approximately 4,000

laboratory analyses were also delayed [*ibid*]. In addition, 150 non-urgent operations were cancelled, and several urgent oncology patients were transferred to other hospitals in Barcelona for treatment continuation [58], [61].

Following the ransomware detonation, the attackers demanded a ransom of $4.5 million for the encrypted data [61], [62]. The HCB and the Catalonia regional government confirmed that they would not negotiate with the attackers or pay the ransom [62].

In addition to system encryption, the cyber-attack also involved the exfiltration and compromise of sensitive data.

According to official briefings issued by the FRCB-IDIBAPS, specific personal data associated with hospital staff and research activities were accessed and copied during the attack [63], [64].

Following investigations, it was confirmed that the compromised data included contact information of current and former staff members. It also included personal data from donors participating in biomedical research programmes [63], [64].

Public reports also indicated that the RansomHouse claimed to have exfiltrated approximately 4.5 terabytes of data from the affected system [65].

Monitoring activities to detect potential publication of stolen data were launched. It was later confirmed that several documents containing personal data were published on the dark web [63].

Following the attack, the HCB and FRCB-IDIBAPS implemented a range of contingency measures to restore operations [63], [64]. Healthcare staff had to rely on manual procedures. At the same time, IT teams worked to contain the intrusion and restore affected systems.

Recovery processes gradually resumed medical activities. Within the first week, approximately 90% of complex surgeries and 70% of outpatient consultations had resumed [57].

In sum, the attack disrupted essential healthcare services and postponed thousands of medical procedures. It also involved confirmed data compromise and a ransom demand against a major public hospital.

4.2.2 Mapping to legal criteria

4.2.2.1 Article 2(a): scope, scale, impact or severity of disruption

Article 2(a) requires an assessment of the scope, scale, impact, or severity of disruption caused, including effects on essential services, critical State functions, public order or public safety.

The ransomware attack targeted a major public health institution providing critical medical services within the Catalan health system.

The incident disrupted several key hospital systems, including electronic medical records, radiology systems, pharmacy operations, and laboratory services. As a result, HCB staff were forced to revert to manual workarounds and paper-based documentation to continue providing medical services [57], [58], [60].

According to public reporting, the cyber-attack resulted in the cancellation of approximately 450 surgical procedures. It also caused the postponement of more than 11,000 outpatient consultations and delays affecting around 4,000 laboratory analyses [57], [58], [61].

In addition, several oncology patients requiring urgent treatment were transferred to other hospitals in Barcelona for care continuity [58], [61].

The disruption also affected external entities connected to the HCB's infrastructure. These included biomedical research organisations and primary care centres sharing the same IT environment [60].

The disruption of essential healthcare services, temporary reliance on manual processes, and the postponement of thousands of medical procedures indicate a substantial operational impact.

On the basis of publicly available evidence, Article 2(a) is plausibly satisfied.

4.2.2.2 Article 2(b): the number of natural or legal persons, entities or bodies affected

Article 2(b) requires the assessment of the number of persons, entities or bodies affected by the cyber-attack.

The cyber-attack directly affected the operations of the HCB and associated research institutions connected to the same IT infrastructure.

Public reporting indicates significant disruption. This included more than 11,000 outpatient consultations, 4,000 delayed laboratory analyses, and hundreds of cancelled surgical procedures [57], [58], [61].

Although the publicly available reporting does not provide a precise number of individuals affected, the scale of disruption suggests that many patients were indirectly affected.

Furthermore, the cyber-attack also affected HCB staff and research personnel whose personal data was compromised.

Since the Regulation does not provide quantitative thresholds, the available evidence suggests that the cyber-attack affected a substantial number of individuals. However, the absence of precise figures limits the assessment of the full scale of affected persons.

On the basis of publicly available evidence, Article 2(b) is plausibly satisfied.

4.2.2.3 Article 2(c): the number of member states concerned

Article 2(c) requires consideration of the number of EU member states directly concerned by the cyber-attack.

Based on publicly available information, the cyber-attack primarily affected the operations of HCB and associated entities in Barcelona. It therefore concerned a healthcare institution operating within a single EU member state.

Although the investigation of the attack involved international law enforcement cooperation, including coordination with Interpol and Europol, the operational disruption itself appears to have been contained within Spain [58].

Since the Regulation does not define a quantitative threshold for this criterion, the HCB cyber-attack can be understood as affecting a single EU member state.

On the basis of publicly available evidence, Article 2(c) is partially satisfied.

4.2.2.4 Article 2(d): the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property

Article 2(d) requires consideration of the amount of economic loss caused by the cyber-attack.

In the context of the HCB cyber-attack, public reporting does not provide a quantified estimate of the financial losses resulting from the incident.

However, the disruption led to measurable economic consequences within a major public healthcare institution. The cancellation and postponement of diagnostic services and medical procedures likely generated indirect financial costs.

In addition, the attack required significant emergency response efforts, including incident response operations, system restoration, and the implementation of contingency measures across the HCB and the FRCB-IDIBAPS [63], [64].

Although public reporting does not quantify the financial cost of these disruptions, the scale of cancelled medical services indicates economic consequences. Post-incident activities also likely generated costs for the HCB and the healthcare system.

On the basis of publicly available evidence, Article 2(d) is partially satisfied.

4.2.2.5 Article 2(e): the economic benefit gained by the perpetrator, for himself or for others

Articles 2(e) requires consideration of the economic benefit gained by the perpetrators as a result of the cyber-attack.

Public reporting indicates that RansomHouse demanded a ransom of $4.5 million to release the encrypted data [60], [61]. However, the HCB and Catalonia regional government stated they would not engage in negotiations or pay the ransom [62].

Since the ransom was not paid, there is no publicly available evidence confirming whether the attackers obtained direct financial gains from the HCB cyber-attack.

Nevertheless, the ransom demand itself highlights a clear financial motivation behind the cyber operation.

On the basis of publicly available evidence, Article 2(e) is partially satisfied.

4.2.2.6 Article 2(f): the amount or nature of data stolen or the scale of data breaches

Article 2(f) requires consideration of the nature and quantity of data stolen, accessed, or otherwise compromised during the cyber-attack.

According to public reporting, the RansomHouse group claimed to have exfiltrated 4.5 terabytes of data from the affected system [61], [64].

Although this figure originates from a statement made by the attackers, subsequent investigations confirmed that certain categories of personal data were accessed and copied. This data was associated with the HCB staff and biomedical research activities [63], [64].

The confirmed data compromise and the reported scale of stolen data indicate that a substantial amount of sensitive and personal data was accessed during the attack.

On the basis of publicly available evidence, Article 2(f) is plausibly satisfied.

4.2.2.7 Article 2(g): the nature of commercially sensitive data accessed

Article 2(g) requires consideration of the nature of commercially sensitive data accessed during the cyber-attack.

Public reporting confirms that the ransomware involved the exfiltration of personal data associated with HCB staff and biomedical research activities conducted by the FRCB-IDIBAPS [63], [64].

The compromised data included contact details of current and former staff personnel, identification information, and personal data linked to donors participating in biomedical research activities [63], [64].

Furthermore, the FRCB-IDIBAPS confirmed that several documents containing personal data were published on the dark web by the attackers [63].

However, the evidence available does not indicate whether proprietary research data, commercial contracts, or other forms of commercially sensitive institutional information were accessed during the attack.

While the exposure of personal and research-related data raises concerns at the GDPR level, the available evidence does not demonstrate that commercially sensitive data was compromised.

On the basis of publicly available evidence, Article 2(g) is not satisfied.

The outcome of mapping the HCB 2023 cyber-attack characteristics against Article 2 criteria of Regulation (EU) 2019/796 is illustrated in Table 3.

4.2.3 Operational challenges identified

The incident-based stress testing of the HCB cyber-attack highlights several operational challenges associated with applying Article 2 criteria of Regulation (EU) 2019/796 using publicly available information.

Similar to the previous case study, the absence of quantitative thresholds within the Regulation complicates the interpretation of several criteria.

Article 2(a) requires consideration of the scope, scale, and severity of disruption caused by the cyber-attack. In the HCB case, the attack disrupted a major public healthcare institution. It resulted in the cancellation of hundreds of surgeries and thousands of outpatient consultations.

While the consequences clearly indicate significant disruption, the Regulation does not define the required magnitude. As a result, the assessment relies on qualitative interpretation.

A second challenge concerns the availability and completeness of publicly reported information. This is relevant when evaluating economic loss under Article 2(d).

In contrast to the HSE case study, where audited financial data was available, HCB public sources do not provide a quantified cost estimates.

Although the disruption of HCB's operations and incident response measures suggests the existence of economic losses, the absence of financial reporting limits the ability to assess this criterion with precision.

A third challenge concerns difficulties in verifying the nature and scale of data exfiltration. This is particularly the case when information originates from statements made by the attackers.

In the HCB case, the ransomware group claimed to have exfiltrated several terabytes of data from the hospital's systems. While personal data compromise was later confirmed, the precise volume and full content of the stolen data remain uncertain.

This creates challenges when applying Article 2(f) and Article 2(g). Both criteria require consideration of the amount and nature of data accessed during the cyber-attack.

Lastly, this case study illustrates the difficulty of distinguishing between personal data breaches and the compromise of commercially sensitive information. While the cyber-attack involved the exposure of personal and research-related data, public reporting does not clearly indicate whether proprietary research data or commercially sensitive institutional information was accessed.

This ambiguity complicates the application of Article 2(g) which refers to commercially sensitive data.

In sum, these observations illustrate that even significant disruption to essential services may be difficult to assess under the Regulation. The practical application of the criteria remains constrained by interpretative ambiguity and limitations in public available evidence. These challenges highlight the difficulties researchers or analysts may face when attempting to assess cyber incidents against the framework using open-source data alone.

4.3 Case study: France Travail data breach

4.3.1 Incident overview and impact

This case study examines a cyber-attack targeting France Travail. France Travail is the French national employment agency responsible for job seeker and unemployment benefits services.

In March 2024, France Travail issued a statement about a cyber-attack involving unauthorised access to its information system and the exfiltration of personal data [66], [67].

According to the French Data Protection Authority (Commission nationale de l'informatique et des libertés, CNIL), the attackers gained access through compromised accounts associated with partner organisations [67].

It is reported that following investigations, the data breach may have been carried out between 6 February and 5 March 2024 [68].

The cyber-attack primarily involved data exfiltration rather than system-wide disruption. There is no public evidence that core service delivery was significantly disrupted. Nevertheless, the scale of the data breach was substantial.

Public reporting indicates that personal data relating to 43 million individuals may have been accessed. This included current and former job seekers registered over a 20-year period [66], [67], [68], [69], [71].

The compromised data included personal information such as names, dates of birth, social security numbers, and contact details. France Travail stated that no passwords or bank details were accessed. [66]

The data breach resulted in regulatory consequences including administrative sanctions concerning data protection and security measures. In January 2026, the CNIL fined France Travail €5 million for failing to ensure the protection and security of job seeker's data [67].

French authorities arrested three individuals on 20 March 2024 on suspicion of involvement in the cyber-attack [69], [70]. The suspects were reportedly based in France. Investigations were opened for charges including illegal access to information systems and data extraction [69].

However, the lack of public reporting on the subsequent criminal procedure creates uncertainty. Publicly available evidence does not conclusively establish whether the attack fulfils the external threat conditions[10] of Article 1.

In sum, the scale of the data breach, the number of individuals potentially affected, and the sensitivity of the compromised data illustrate why this case is relevant. It provides a relevant scenario for assessing the applicability of Article 2 of Regulation (EU) 2019/796.

4.3.2 Mapping to legal criteria

4.3.2.1 Article 2(a): scope, scale, impact or severity of disruption

Article 2(a) requires an assessment of the scope, scale, impact, or severity of disruption caused, including effects on essential services, critical State functions, public order or public safety.

The cyber-attack against France Travail primarily involved large-scale data exfiltration rather than operational disruption. There is no publicly available evidence suggesting otherwise.

However, the scale of the incident is substantial. This is due to the volume of data accessed and the number of individuals affected.

According to public reporting, personal data concerning 43 million individuals may have been accessed [66], [67], [68], [69], [71].

While the absence of operational disruption limits the immediate impact on service continuity, the societal implications of such a large-scale data breach are significant. The exfiltration of personal data may generate long-term risks for the affected individuals, including fraud and identity theft.

On the basis of publicly available evidence, Article 2(a) is partially satisfied.

[10] Article 1 defines cyber-attacks constituting an external threat as those that originate from outside the Union, use infrastructure located outside the Union, or are conducted within the support or direction of such actors

4.3.2.2 *Article 2(b): the number of natural or legal persons, entities or bodies affected*

Article 2(b) requires the assessment of the number of persons, entities or bodies affected by the cyber-attack.

Public reporting indicates that the cyber-attack may have affected personal data concerning 43 million individuals. This included current and former job seekers registered with France Travail over approximately 20 years [66], [67], [68], [69], [71].

Open-source information does not distinguish between individuals whose data was accessed and those whose data may have been potentially exposed. As a result, the precise number of directly affected individuals cannot be conclusively determined.

Despite this limitation, the scale of the dataset involved strongly indicates that a significant number of individuals were affected.

On the basis of publicly available evidence, Article 2(b) is plausibly satisfied.

4.3.2.3 *Article 2(c): the number of member states concerned*

Article 2(c) requires consideration of the number of EU member states directly concerned by the cyber-attack.

Based on publicly available information, the cyber-attack targeted a national public administration system within France. There is no evidence indicating that systems or entities in other EU member states were directly affected.

While the data breach concerns a large number of individuals, the attack appears to have been geographically contained within a single member state.

Since the Regulation does not define a quantitative threshold for this criterion, the France Travail cyber-attack can be understood as affecting a single EU member state.

On the basis of publicly available evidence, Article 2(c) is partially satisfied.

4.3.2.4 *Article 2(d): the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property*

Article 2(d) requires consideration of the amount of economic loss caused by the cyber-attack.

Open-source information does not provide a quantified estimate of the economic losses caused by the cyber-attack on France Travail.

While the attack resulted in regulatory consequences, the CNIL fine reflects regulatory enforcement but it does not represent direct economic loss caused by the attack itself.

Lastly, there is no publicly available evidence quantifying costs related to incident response, system remediation, or broader economic impact.

On the basis of publicly available evidence, Article 2(d) is not satisfied.

4.3.2.5 Article 2(e): the economic benefit gained by the perpetrator, for himself or for others

Articles 2(e) requires consideration of the economic benefit gained by the perpetrators as a result of the cyber-attack.

Publicly available reporting does not indicate that a ransom demand was made or that the perpetrators obtained a direct financial gain from the cyber-attack.

While the unauthorised access to personal data may potentially lead to illicit activities, there is no publicly available evidence confirming that financial benefits were realised.

On the basis of publicly available evidence, Article 2(e) is not satisfied.

4.3.2.6 Article 2(f): the amount or nature of data stolen or the scale of data breaches

Article 2(f) requires consideration of the nature and quantity of data stolen, accessed, or otherwise compromised during the cyber-attack.

Public reporting indicates that the compromised data included personal identification data such as names, dates of birth, social security numbers, and contact information [66], [67]. This type of data is considered sensitive, especially in the context of the GDPR.

Although no financial data or passwords were reportedly accessed [66], the exposure of personal data significantly increases the risk of fraud and identity theft.

On the basis of publicly available evidence, Article 2(f) is plausibly satisfied.

4.3.2.7 Article 2(g): the nature of commercially sensitive data accessed

Article 2(g) requires consideration of the nature of commercially sensitive data accessed during the cyber-attack.

In the France Travail data breach, publicly available information highlights that the cyber-attack involved personal data relating to individuals.

There is no evidence suggesting that commercially sensitive data was accessed. This includes proprietary business information or strategic institutional data.

Based on the publicly available evidence, Article 2(g) is not satisfied.

The outcome of mapping the France Travail cyber-attack characteristics against Article 2 criteria of Regulation (EU) 2019/796 is illustrated in Table 4.

4.3.3 Operational challenges identified

The incident-based stress testing of France Travail cyber-attack highlights several operational challenges associated with applying the Article 2 legal criteria of Regulation (EU) 2019/796 to cyber-attacks using publicly available information.

The case study illustrates the limited applicability of disruption-based criteria.

Article 2(a) places emphasis on the scope, scale, and severity of the disruption. This is relevant in relation to essential services and societal activities.

However, the France Travail cyber-attack primarily involved large-scale data exfiltration without observable disruption to core service delivery. While the societal impact of the data breach is significant, the absence of operational disruption limits the assessment. This constrains the extent to which Article 2(a) can be conclusively satisfied.

Furthermore, the cyber-attack exposes ambiguity in assessing the number of persons affected.

Public reporting indicates that 43 million individuals may have been affected [66], [67], [68], [69], [71]. It remains unclear how many persons were directly affected as opposed to potentially exposed.

The lack of distinction between confirmed and potential impact introduces uncertainty in the application of Article 2(b), especially in the absence of defined thresholds.

In addition, the absence of quantified economic loss presents a significant evidentiary limitation.

Article 2(d) requires consideration of the economic impact of a cyber-attack. Although a €5 million administrative fine was imposed on France Travail by the CNIL [67], there is no public evidence of the direct or indirect losses resulting from the cyber-attack.

Costs related to incident response, remediation, or long-term consequences are not quantified, which limits the ability to assess this criterion consistently.

The case study also highlights limitations in the categorisation of data types under Article 2(f) and Article 2(g).

While the compromised data clearly includes sensitive personal information, the Regulation does not clearly distinguish personal data from commercially sensitive data. This creates interpretative challenges when applying these criteria to large-scale public sector datasets.

Lastly, the case study identifies a broader dependence on open-source information.

Public reporting provides limited visibility into the operational, technical, and financial dimensions of the cyber-attack. As a result, the assessment relies on partial or sometimes ambiguous evidence, reinforcing the interpretative nature of the analysis.

To conclude, these challenges illustrate that Article 2 provides a flexible framework for assessing cyber-attacks. However, its application to data breach incidents remains constrained by ambiguity, lack of thresholds, and limited open-source evidence.

Considering RQ1: "To what extent can the EU cyber sanctions framework's criteria be operationalised using publicly available information on cyber-attacks?"

The case study analysis conducted in this chapter highlights that the EU cyber sanctions framework's criteria can be operationalised to a certain extent using publicly available information. But not without significant limitations.

The application of Article 2 criteria across the selected case studies shows that observable characteristics of cyber-attacks can be mapped against the framework using qualitative indicators.

In particular, criteria concerning the scope of disruption, Article 2(a), number of affected persons, Article 2(b), and the nature of data accessed, Article 2(f) can be assessed based on open-source reporting.

However, the findings also reveal significant constraints. Several criteria cannot be consistently evaluated due to the absence of reliable and quantified data in public sources.

These criteria include the economic loss caused by the cyber-attack, Article 2(d), and the economic benefit gained by perpetrators, Article 2(e).

In addition, the operationalisation of Article 1 of (EU) Regulation 2019/796 remains inherently limited. This is because verification of the external threat dimension depends on attribution elements that may not be available in open-source information.

Although the framework can be applied in a structured and comparable manner, its full operationalisation cannot be achieved without reliance on information available beyond the public domain.

Considering RQ2: "How do selected cyber-attacks affecting the EU since 2019 map against the framework's criteria for identifying an attack with a significant effect?"

The mapping of selected cyber-attacks illustrates that the extent to which Article 2 factors are satisfied varies considerably depending on the nature of the attack itself.

Ransomware attacks affecting critical infrastructure, such as the HSE and HCB cases, show a different pattern of alignment. Criteria related to the number of affected persons and the nature of data accessed are strongly engaged. By contrast, economic loss to the affected entity and economic benefit to perpetrators remain difficult to assess.

This variation highlights that the framework does not apply uniformly across different types of malicious cyber operations. Instead, its criteria appear more readily applicable to disruptive attacks than to large-scale data breaches.

This reveals variation in how the concept of cyber-attack with a "*significant effect*" is operationalised across different types of cyber operations.

To conclude, these findings provide the basis for the analytical discussion in Chapter 5. The discussion will further examine the operational and evidentiary challenges identified, and their implications for the operational applicability of the EU cyber sanctions framework.

5 Cross-case analysis

This chapter builds on the findings of Chapter 4 by conducting a cross-case analysis of the selected cyber-attacks vis-à-vis the EU cyber sanctions framework.

The previous chapter assessed each case individually against Article 2 of Regulation (EU) 2019/796. This chapter adopts a comparative perspective. It identifies recurring patterns, operational challenges, and variations in the application of these criteria across the selected cyber operations.

This chapter addresses the following research questions:

- RQ3: Which criteria within the EU cyber sanctions framework present the greatest practical challenges when applied to contemporary cyber operations?
- RQ4: What limited clarifications or adjustments to the framework's criteria could improve their operational applicability?

The analysis focuses on the practical usability of the framework, examining both its strengths and limitations when applied on the basis of publicly available information.

This approach is divided into three steps. First, it identifies recurring operational challenges across the case studies. Second, it examines these challenges at the level of individual Article 2 criteria. Third, it considers their implications for the framework's operational usability.

5.1 Recurring operational challenges

The cross-case analysis shows that several operational challenges arise consistently across different types of cyber-attacks.

These challenges limit the practical application of the framework when relying on publicly available information. They are not case specific but reflect structural characteristics of the EU cyber sanctions framework itself.

A first recurring challenge concerns the absence of quantitative thresholds within Article 2 criteria.

The Regulation does not define minimum thresholds for key criteria. These include the scale of disruption, number of affected persons, and level of economic loss required to constitute a ***significant effect***.

As observed across all case studies, this absence requires a qualitative and interpretative assessment. This introduces subjectivity and reduces consistency across cases.

For example, both the HSE and France Travail cases involved large-scale impacts. However, the criteria are satisfied through different dimensions.

In the HSE case, the relevant dimension is disruption. In the France Travail, it is data exposure. There is no clear benchmark for comparison.

A second recurring challenge relates to the limited availability of reliable economic impact data.

Article 2(d) and Article 2(e) require consideration of economic loss to the target and economic benefit gained by the perpetrator. However, across the case studies, this information is either incomplete, not quantified, or entirely absent in publicly available sources.

The HSE case provides partial cost estimates. By contrast, the attacks targeting HCB and France Travail lack detailed economic impact information.

Similarly, there is no verifiable information regarding whether the perpetrators gained financial benefit. This is especially evident in the France Travail case, where no ransom demand was reported.

This significantly constrains the consistent application of these criteria.

A third challenge concerns the uneven applicability of the framework across different types of cyber operations.

The case studies demonstrate that the criteria are more readily applicable to disruptive ransomware attacks than to incidents primarily involving data exfiltration.

In ransomware cases, such as the HSE and HCB, multiple criteria can be clearly observed. These include scope of disruption, economic impact, and operational consequences.

In contrast, the France Travail data breach strongly engages criteria related to the number of affected persons and the nature of data accessed. It leaves other criteria difficult to assess.

This suggests that the EU cyber sanctions framework does not capture all forms of cyber-attack impact with equal effectiveness.

Lastly, all case studies highlight a broader dependence on publicly available information, introducing limitations in terms of completeness, reliability, and comparability.

Public reporting often lacks quantified impact, technical details, and consistent terminology. As a result, the assessment of criteria remains partially interpretative and subject to evidentiary gaps, limiting the reproducibility of the analysis.

In addition to the challenges identified at the level of Article 2 indicators, the analysis highlights a specific limitation concerning the operationalisation of Article 1.

Article 1 defines the scope of the Regulation by requiring that cyber-attacks constitute an external threat to the EU. This requirement was not assessed at the level of individual case studies. This is because conclusive attribution was not available in public sources.

The verification of whether a cyber-attack originates from outside the EU, involves infrastructure located outside the Union, or is carried out by actors operating outside the Union requires attribution elements. These elements are not consistently observable in open-source information.

This limitation is illustrated by the France Travail case. French authorities reportedly arrested suspects in connection with the cyber-attack. However, these developments do not establish whether the attack fulfils the external threat conditions under Article 1.

Publicly available information does not clarify whether the attack involved external infrastructure or actors operating outside the EU.

As a result, Article 1 functions as a condition to define the scope of a cyber-attack. However, it cannot always be empirically validated within the analytical framework used in this research.

This creates a structural constraint as the applicability of the Regulation depends partly on criteria that cannot be operationalised through public information alone.

In sum, these recurring challenges indicate that the main obstacles do not derive from the selected cyber-attacks themselves. They arise from the interaction between broadly framed legal criteria and uneven public evidence.

The next section therefore moves from cross-case level to the indicator level analysis. It identifies which Article 2 criteria are more usable, partially usable, or difficult to operationalise.

5.2 Indicator-level assessment

The analysis identifies that the practical applicability of the framework varies significantly at the level of individual indicators.

Some Article 2 criteria can be applied consistently. Others present persistent operational and evidentiary challenges.

To support the cross-case assessment, Table 1 provides a high-level overview of how each Article 2 criterion was analysed.

The full mapping of the selected cyber-attacks against Article 2 is available in Appendix 3.

Table 1: High-level overview of the case study assessment at the indicator level.

Article 2 criteria	***Health Service Executive (HSE)***	***Hospital Clínic de Barcelona (HCB)***	***France Travail***
(a) Scope, scale, impact	Plausibly satisfied	Plausibly satisfied	Partially satisfied
(b) Number of persons affected	Plausibly satisfied	Plausibly satisfied	Plausibly satisfied

(c) Number of member states affected	Partially satisfied	Partially satisfied	Partially satisfied
(d) Economic loss	Plausibly satisfied	Partially satisfied	Not satisfied
(e) Economic benefit gained by perpetrator	Partially satisfied	Partially satisfied	Not satisfied
(f) Nature of data	Plausibly satisfied	Plausibly satisfied	Plausibly satisfied
(g) Commercial data	Partially satisfied	Not satisfied	Not satisfied

As illustrated in Table 1, the application of Article 2 criteria varies significantly across cases.

Criteria related to disruption and economic loss, such as Articles 2(a) and 2(d), are more readily satisfied in ransomware scenarios affecting critical or essential infrastructure.

In contrast, data breach incidents, such as France Travail, primarily engage criteria related to the number of affected persons and the nature of data accessed. Operational and economic indicators remain more difficult to assess.

The table further highlights that certain criteria, including Article 2(c), are consistently assessed as partially satisfied. This indicates limited differentiation across cases.

Similarly, Articles 2(d) and 2(e) show the greatest variability. They are most often partially satisfied or not satisfied. This reinforces their limited operational applicability in open-source analysis.

This indicator-level variation is important because it refines the broader patterns identified in Section 5.1. Rather than showing that the framework is simply usable or unusable, it shows uneven operational applicability across the criteria.

The following subsections distinguish between three groups of criteria. These are criteria with partial operational applicability, criteria that are difficult to operationalise, and criteria affected by conceptual ambiguity.

5.2.1 Article 2 criteria with partial operational applicability

The analysis identifies that certain Article 2 criteria demonstrate partial operational applicability when assessed using publicly available information.

This applies particularly to Article 2(a) and Article 2(c). The Articles relates to the scope, scale, and severity of disruption, and the number of member states affected, respectively.

Article 2(a) can be applied with relative clarity in cases where cyber-attacks result in observable disruption to essential services. This is evident in ransomware attacks such as the HSE and HCB cases, where service outages, delays in medical treatment, and operational disruption are clearly documented.

However, its application becomes less straightforward in cyber-attacks primarily involving data exfiltration.

In the France Travail case, while the scale of the data breach was significant, the absence of observable disruption limits the extent to which this criterion can be fully satisfied.

Similarly, Article 2(c) is consistently assessed as partially satisfied across all case studies. While it is possible to determine whether a cyber-attack is contained within a single EU member state, the absence of defined thresholds or further guidance limits its analytical value. In practice, this criterion does not meaningfully differentiate between cases, as it does not capture the qualitative significance of cross-border impact.

In sum, these criteria can be applied in a structured manner but do not provide strong analytical differentiation across cases.

5.2.2 Article 2 criteria that are difficult to operationalise

The analysis further identifies a group of criteria that are consistently difficult to operationalise using publicly available information.

These include Article 2(d), relating to economic loss to the affected institution, and Article 2(e), concerning the economic benefit gained by the perpetrator.

Across all case studies, the assessment of economic loss is constrained by the absence of reliable and comprehensive financial data.

While the HSE case provides partial cost estimates, these figures remain incomplete. In contrast, the HCB and France Travail cases lack public evidence on quantified economic impact altogether.

Similarly, the assessment of economic benefit gained by the perpetrator is not supported by observable evidence. In the absence of confirmed ransom payments or verified monetisation of stolen data, it is not possible to determine whether financial gain was realised.

This is particularly evident in the France Travail case, where no ransom demand was reported.

As a result, these criteria cannot be applied consistently and introduce a high degree of uncertainty into the assessment. Consequently, their operational applicability is significantly limited in an open-source analytical context.

5.2.3 Article 2 criteria with conceptual ambiguity

In addition to evidentiary limitations, certain criteria present challenges due to conceptual ambiguity.

Article 2(g), relating to the nature of commercially sensitive data accessed, is particularly affected by this limitation.

The Regulation does not provide a clear definition of commercially sensitive data. It also does not explain how this category should be distinguished from other types of sensitive information. This creates uncertainty in its application.

In the case studies analysed, large volumes of sensitive personal data were accessed, particularly in the HSE and France Travail cases.

Although such data may carry significant societal and financial risks, it does not clearly fall within a distinct category of commercially sensitive data as defined by the Regulation.

In sum, the application of Article 2(g) depends primarily on interpretation, which limits consistency and reduces its analytical value.

To conclude, the indicator-level assessment shows that the framework's limitations are not uniform. Some criteria can be applied with relative structure. Some are difficult to evidence, while others suffer from conceptual ambiguity.

This distinction matters because it does not point to one single deficiency. Instead, it points to different operational weaknesses requiring different forms of clarification.

The next section turns from diagnosis to implication. It considers what these findings mean for operational usability and where targeted adjustments could improve application.

5.3 Implications for operational usability

The findings of this study indicate that the EU cyber sanctions framework provides a flexible structure for assessing cyber-attacks. However, its practical application is constrained by ambiguity, lack of thresholds, and evidentiary limitations.

These challenges do not necessarily require a fundamental revision of the framework. Targeted clarifications could improve operational usability, especially where assessments rely on public information.

An alternative interpretation is that these challenges do not necessarily indicate weaknesses in Regulation (EU) 2019/796 itself. The absence of robust thresholds may be intentional. It allows decision-makers to retain flexibility when assessing diverse cyber operations. In addition, EU institutions may rely on classified intelligence and confidential assessments unavailable to external researchers.

Therefore, some limitations identified in this study may reflect open-source analysis constraints rather than deficiencies in the legal framework.

A first implication concerns the relationship between Article 1 and Article 2 of Regulation (EU) 2019/796.

Article 1 defines the scope of the Regulation. It applies to cyber-attacks with a ***significant effect*** **that constitute an external threat** to the EU or its member states.

It further specifies that such external threats include cyber-attacks originating from outside the Union. They may also involve infrastructure located outside the Union, or are carried out by actors operating outside the EU, or under their direction [2].

However, while Article 1 introduces the requirement of a "*significant effect*", it does not provide criteria for determining when this threshold is met. This assessment is carried out implicitly through Article 2 factors.

As demonstrated across the case studies, the link between Article 1 and Article 2 is implicit rather than operationalised.

The Regulation does not clarify how the criteria of Article 2 should be interpreted in order to determine whether a cyber-attack meets the threshold of *significant effect* under Article 1.

To improve operational usability, the framework could benefit from clearer guidance on how Article 2 criteria contribute to this assessment. This could include structured interpretative guidance or indicative benchmarks supporting consistent application. Such guidance should preserve the flexibility of the framework.

A second implication concerns the interpretation of the criteria set out in Article 2.

As demonstrated across the case studies, the absence of indicative thresholds requires decision-makers to rely on qualitative judgment when assessing factors such as the scale of disruption, the number of affected persons, or the level of economic impact.

While this flexibility allows the framework to accommodate a wide range of cyber operations, it also introduces subjectivity. It may also limit consistency across cases.

Similar levels of impact may be interpreted differently depending on whether disruption, data exposure, or economic consequences are emphasised.

To address this, the framework could benefit from non-binding interpretative guidance supporting consistent application of Article 2 criteria. This could include indicative

reference points or structured assessment approaches. It should not establish strict thresholds.

A third implication relates to the assessment of economic loss and economic benefit gained by the perpetrator under Articles 2(d) and 2(e) respectively.

The analysis demonstrates that these criteria are among the most difficult to operationalise due to the limited availability of reliable and comprehensive financial data.

As illustrated in the HSE case, direct costs may sometimes be estimated. However, indirect costs such as staff time and operational disruption are not fully quantified. Long-term expenditures may also remain projected or uncertain.

In the HCB and France Travail cases, publicly available information does not provide quantified economic data.

Similarly, the economic benefit gained by perpetrators is rarely observed. Without confirmed ransom payments or evidence of monetisation, this criterion remains speculative.

To improve operational applicability, the framework could incorporate qualitative indicators of economic impact. This would allow assessments to account for broader economic consequences where precise quantification is not available.

A fourth implication concerns the interpretation of data-related criteria, such as Article 2(f) and Article 2(g).

Although the nature of accessed data can generally be identified via public reporting, the Regulation does not clearly define or distinguish between different categories of data. In particular, the concept of "commercially sensitive data" is undefined.

Large-scale data breaches involving sensitive personal data may have significant societal and financial implications. However, they do not clearly fall within the category of commercially sensitive data under the Regulation.

This creates interpretative uncertainty and limits consistency in the application of Article 2(g), related to the nature of commercially sensitive data accessed.

To address this, the framework could benefit from a clearer categorisation or examples of data types. This would support a more consistent and transparent assessment.

A fifth implication relates to evidentiary limitations associated with publicly available information.

The analysis demonstrates that several criteria, particularly those relating to economic impact and attribution, cannot be fully assessed using open-source data alone.

This limitation is evident in relation to Article 1. As illustrated in the France Travail case, suspects may be identified, and legal proceedings may be initiated. However, publicly available information may still not establish whether the attack meets the Regulation's external threat conditions.

In addition, the assessment of certain elements may depend on ongoing legal or investigative processes. Relevant information may therefore become available only after significant delays.

This creates a temporal constraint. Decision-makers may not be able to fully apply the framework within a timeframe that supports timely policy responses.

This suggests that the application of the framework may rely on information outside the public domain. It may also depend on the completion of legal or investigative procedures. Consequently, the operational use of the framework may be inherently limited in fast-evolving cyber-attack contexts.

To improve transparency, the framework could benefit from explicitly acknowledging these constraints. It could also clarify how assessments may be conducted when information is incomplete, evolving, or dependent on ongoing legal procedures.

Finally, the analysis highlights that the framework does not apply uniformly across different types of cyber operations.

The framework appears to be more readily applicable to disruptive ransomware attacks than to incidents involving data exfiltration or limited observable impact.

This uneven applicability suggests that the concept of "*significant effect*" is more closely aligned with disruption-based scenarios.

As a result, the impact of large-scale data breaches may be underrepresented.

To address this, the framework could incorporate greater recognition of non-disruptive forms of impact, including long-term risks associated with data exposure and societal consequences. This would ensure that the framework remains relevant in the context of evolving cyber threats.

In sum, these findings indicate that the EU cyber sanctions framework is operationally applicable, but not without limitations. Rather than requiring structural reform, it would benefit from targeted clarifications. These could improve consistency, reduce ambiguity, and better reflect the evolving nature of cyber operations.

The proposed adjustments would enhance the framework's usability as an analytical and policy tool. At the same time, they would preserve the flexibility needed to address diverse cyber threats.

6 Conclusion

This study examined the operational applicability of the EU cyber sanctions framework. It focused on the criteria established in Regulation (EU) 2019/796 for identifying cyber-attacks with a significant effect.

The research was based on three case studies and an incident-based stress testing approach. This approach allowed the framework to be assessed against observable characteristics of real cyber-attacks.

The findings show that the framework can be applied using publicly available information, but only to a certain extent.

Some Article 2 criteria can be assessed with relative consistency, especially those relating to the number of persons affected and the nature of the data involved. These elements are often documented in public reporting and allow for a reasonably structured assessment.

However, other criteria are significantly more difficult to operationalise.

This is especially true for Article 2 criteria related to economic loss suffered by the affected institution, and the economic benefit gained by the perpetrators. It also applies to Article 1 elements relating to attribution and the external dimension of a cyber-attack.

Across all case studies, these aspects were either partially observable or not sufficiently supported by open-source information. As a result, the assessment relies on interpretation rather than clearly defined indicators.

The mapping of the selected cyber-attacks further shows that the framework does not apply evenly across different types of malicious cyber operations.

Disruptive ransomware attacks affecting critical and essential infrastructure tend to engage a broader range of Article 2 criteria. In contrast, large-scale data breaches primarily engage criteria related to scale and data exposure.

This creates an uneven analytical landscape, in which some cyber-attacks can be assessed more comprehensively than others.

In the case studies analysed, ransomware attacks engaged more Article 2 criteria because they combined service disruption, ransom demands, and documented costs. In contrast, the France Travail data breach primarily provided evidence of data exposure and affected persons. Unlike ransomware, data breaches do not necessarily disrupt operations, as the affected systems and data can remain available and usable by the affected entity.

Furthermore, the cross-case analysis identifies several recurring operational challenges. These include the absence of quantitative thresholds, the limited availability of financial loss information, and a broader dependence on inconsistent or incomplete public reporting.

In addition, the relationship between Article 1 and Article 2 is difficult to operationalise in practice. Article 1 defines the scope of the Regulation and requires that cyber-attacks constitute an external threat. However, these conditions cannot be conclusively assessed using open-source information alone.

This limitation is further reinforced by the role of legal processes. As illustrated in the France Travail case, relevant information may only become available over time. It may also depend on ongoing legal procedures.

This creates a temporal constraint, as the applicability of the framework cannot always be assessed within a timeframe that supports timely EU decision-making.

More broadly, the most significant limitation of this study is its reliance on publicly available information. This also limits the incident-based stress testing methodology, which depends on interpretative judgment and a small number of case studies. These weaknesses were mitigated through predefined legal criteria, consistent indicators, and multiple sources.

Based on these findings, this research identifies several targeted clarifications that could improve the framework's operational usability.

These include interpretative guidance for applying the Article 2 criteria and clarification of the relationship between Article 1 and Article 2. They also include explicit acknowledgment of the evidentiary and procedural constraints associated with open-source analysis.

Overall, the framework is sufficiently flexible to accommodate a broad range of cyber operations, but this flexibility introduces ambiguity and limits consistency in its application.

This study demonstrates how the EU cyber sanctions framework performs when applied to contemporary cyber-attacks using publicly available information. It also identifies areas where the operational clarity could be improved.

The analytical framework developed in this study may serve as a baseline for future research and for professionals seeking to assess the operational applicability of cyber sanctions in specific cases.

Recent developments, including the imposition of additional cyber sanctions in March 2026, confirm the continued relevance of the framework. At the same time, the findings of this study suggest that its practical application remains constrained by structural and evidentiary limitations.

These limitations are likely to persist as the cyber threat landscape continues to evolve.

References

[1] Council of the European Union, “Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")”, 10474/17, Brussels, 2017.

[2] Council of the European Union, “Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States”, ST/7302/2019/INIT, Brussels, 2019.

[3] Council of the European Union, “Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States”, ST/7299/2019/INIT, Brussels, 2019.

[4] Council of the European Union, “Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States”, ST/9564/2020/INIT, Brussels, 2020.

[5] Council of the European Union, “Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States”, OJ L 351I, Brussels 2020.

[6] Council of the European Union, “Council Decision (CFSP) 2024/1779 of 24 June 2024 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyberattacks threatening the Union or its Member States (including a list of sanctioned individuals)”, OJ L, 2024/1779, Brussels 2024.

[7] Council of the European Union, “Council Decision (CFSP) 2025/171 of 27 January 2025 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (including the details of the individuals sanctioned today)”, OJ L, 2025/171, Brussels 2025.

[8] Council of the European Union, “Council Decision (CFSP) 2026/588 of 16 March 2026 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States”, OJ L, 2026/588, Brussels 2026.

[9] F. Giumelli, “The success of sanctions: lessons learned from the EU experience”, Farnham: Ashgate, 2013.

[10] D. Cortright, G.A. Lopez, “Smart Sanctions: Targeting Economic Statecraft”, Lanham, MD: Rowman & Littlefield, 2002.

[11] F. Giumelli, "How EU sanctions work: A new narrative", Chaillot papers 129, 2013.

[12] R.A. Pape, “Why economic sanctions do not work”, International security, 22(2), 90-136, 1997.

[13] K.A. Elliott, “The Sanctions Glass: Half Full or Completely Empty?” International Security 23(1), 50-65, 1998.

[14] Baldwin, D. A. 1998. “Evaluating Economic Sanctions.” International Security 23(2), 189-195, 1998.

[15] G.C. Hufbauer, J.J. Schott, K.A. Elliott, B. Oegg, “Economic Sanctions Reconsidered: History and Current Policy”, Washington, D.C: Patterson Institute for International Economics, 2007.

[16] D. Peksen, “When do imposed economic sanctions work? A critical review of the sanctions effectiveness literature”, Defence and Peace Economics, 30(6), 635-647, 2019.

[17] M. Doxey, “Economic Sanctions and International Enforcement”, New York: Oxford

[18] G.C. Hufbauer, J.J. Schott, K.A. Elliott, “Economic sanctions reconsidered: History and current policy”, Vol. 1, Peterson Institute, 1990.

[19] N. A. Bapat, T. Heinrich, Y. Kobayashi, T.C. Morgan, “Determinants of sanctions effectiveness: Sensitivity analysis using new data”, International Interactions, 39(1), 79-98, 2013.

[20] N.A. Bapat, T.C. Morgan, “Multilateral versus unilateral sanctions reconsidered: A test using new data”, International Studies Quarterly, 53(4), 1075-1094, 2009.

[21] W.H. Kaempfer, A.D. Lowenberg. “Unilateral versus Multilateral International Sanctions: A Public Choice Perspective”, International Studies Quarterly, 43(1), 37-58, 1999.

[22] T.C. Morgan, L.V. Schwebach, “Economic Sanctions as an Instrument of Foreign Policy: The Role of Domestic Politics”, International Interactions 21(3), 247-263, 1996.

[23] L. Jones, C. Portela, “Evaluating the success of international sanctions: a new research agenda”, Revista CIDOB d’Afers Internacionals, 125, 39-60, 2020.

[24] F. Giumelli, F. Hoffmann, A. Książczaková, “The when, what, where and why of European Union sanctions”, European Security, 30(1), 1-23, 2021.

[25] C. Portela, “European Union sanctions and foreign policy: when and why do they work?”, Milton Park: Routledge, 2010.

[26] F. Giumelli, “Coercing, constraining and signalling. Explaining UN and EU sanctions after the Cold War”, Colchester: ECPR Press, 2011.

[27] A. Vines, “The effectiveness of UN and EU sanctions: lessons for the twenty-first century”, International affairs, 88 (4), 867–877, 2012.

[28] D. A. Baldwin, “The sanctions debate and the logic of choice”, International security, 24(3), 80-107, 2000.

[29] “Consolidated version of the Treaty on European Union”, OJ C 326, 2012.

[30] “Consolidated version of the Treaty on the Functioning of the European Union”, OJ C 326, 2012.

[31] A. Kozlowski, “The European Union Effective System of Sanctions Against Cyberattacks”, The VISIO JOURNAL, 9, 2018.

[32] Y. Miadzvetskaya, “Challenges of the Cyber Sanctions Regime Under Common Foreign and Security Policy (CFSP)”, Anton Vedder, Jessica Schroers, Charlotte Ducuing, Peggy Valcke, KU Leuven Centre for IT & IP Law Series, 7, 2019.

[33] E. Kapsokoli, “Sanctions and Cyberspace: The Case of the EU's Cyber Sanctions Regime”, In European Conference on Cyber Warfare and Security, 492-XII, Academic Conferences International Limited, 2021.

[34] G.A., Bowen, “Document analysis as a qualitative research method” Qualitative research journal 9, no. 2, 27-40, 2009.

[35] Basel Committee on Banking Supervision, “Stress testing principles”, 2018. Retrieved from: https://www.bis.org/bcbs/publ/d450.pdf

[36] European Central Bank, “Macroprudential stress-tests and tools for the non-bank sector”, (2017). Retrieved from: https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp170922_3.en.html

[37] Stiftung Wissenschaft und Politik, European Repository of Cyber Incidents (EuRepoC). Retrieved from: https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc

[38] PricewaterhouseCoopers (PwC), “Conti cyber attack on the HSE: Independent Post Incident Review”, (2021). Retrieved from: https://www.lenus.ie/entities/publication/1bd0b513-9ffb-4b6f-94f4-cf68116c1e89

[39] Office of the Comptroller and Auditor General, “12. Financial impact of cyber security attack”, (*s.a.*). Retrieved from: https://www.audit.gov.ie/en/find-report/publications/2022/12-financial-impact-of-cyber-security-attack.pdf

[40] Abrams, L. “Conti ransomware gives HSE Ireland free decryptor, still selling data”, (2021). Retrieved from: https://www.bleepingcomputer.com/news/security/conti-ransomware-gives-hse-ireland-free-decryptor-still-selling-data/

[41] Noonan, L. “Ireland examines decryption key to restore health systems after ransomware attack”, (2021). Retrieved from: https://www.ft.com/content/39458539-f206-46fe-83fc-bc14457c699a

[42] Blaney, A. “HSE cyber-attack – which hospitals are affected? Here is everything you need to know”, (2021). Retrieved from: https://www.independent.ie/irish-news/hse-cyber-attack-which-hospitals-are-affected-here-is-everything-you-need-to-know/40432288.html

[43] Health Service Executive, “If you received a letter about the cyber-attack on the HSE”, (2025). Retrieved from: https://www2.hse.ie/services/cyber-attack/received-letter/

[44] Health Service Executive, “HSE cyber-attack – staff information”, (*s.a.*). Retrieved from: https://healthservice.hse.ie/staff/procedures-guidelines/data-protection/hse-cyber-attack-staff-information/

[45] Houses of the Oireachtas, Parliamentary question No. 1369, (2023). Retrieved from: https://www.oireachtas.ie/en/debates/question/2023-01-18/1369/

[46] Health Service Executive, “Cyber-attack and HSE response”, (*s.a.).* Retrieved from: *https://www2.hse.ie/services/cyber-attack/what-happened/*

[47] Horgan-Jones, J., Wall, M. “HSE cyberattack: More than 100,000 people whose personal data stolen to be contacted”, (2022). Retrieved from: https://www.irishtimes.com/health/2022/11/07/over-100000-people-whose-personal-data-stolen-in-hse-cyberattack-to-be-contacted/

[48] O'Donovan, B.(a), “HSE cyber attack: 32,000 notified of stolen data”, (2023). Retrieved from: https://www.rte.ie/news/business/2023/0209/1355572-pac-hse-cyberattack/

[49] Health Service Executive, “Question from Deputy Paul Murphy – PQ 1512-26”, (2026). Retrieved from: https://about.hse.ie/publications/question-from-deputy-paul-murphy-pq-1512-26/

[50] O'Donovan, B.(b), “District Court to hear motions relating to victims of HSE cyber attack”, (2026). Retrieved from: https://www.rte.ie/news/business/2026/0225/1560419-cork-court-to-hear-motions-relating-to-hse-cyber-attack-victims/

[51] Irish Information Security Forum, “HSE systems breached in new Cyberattack”, (*s.a.*). Retrieved from: https://www.iisf.ie/HSE-systems-breached-again

[52] Foreign, Commonwealth & Development Office, “UK cracks down on ransomware actors”, (2023). Retrieved from: https://www.gov.uk/government/news/uk-cracks-down-on-ransomware-actors

[53] Law Society Gazette Ireland, “HSE facing 473 lawsuits after Russian cyber attack”, (2024). Retrieved from: https://www.lawsociety.ie/gazette/top-stories/2024/may/hse-facing-473-lawsuits-after-russian-cyber-attack

[54] O'Donovan, B.(c), “More than 470 legal actions taken against HSE over cyber-attack”

[55] Bowers, S. “HSE offers €750 to victims of system-wide cyberattack”, (2025). Retrieved from: https://www.irishtimes.com/health/2025/12/09/hse-offers-750-to-victims-of-system-wide-cyberattack/

[56] Clínic Barcelona(a), “Statement on the computer attack on the FRCB-IDIBAPS 29/03/2023”, (2023), Retrieved from: https://www.clinicbarcelona.org/en/news/computer-attack-on-the-frcb-idibaps

[57] Jordan, G., “Cybercriminals demand $4.5m ransom from Hospital Clínic”, (2023). Retrieved from: https://www.catalannews.com/tech-science/item/cybercriminals-demand-45mransom-from-hospital-clinic

[58] Hoplon infosec, “A Hospital Clinic Was Under Ransomware Attack in March 2023 in Barcelona”, (2025). Retrieved from: https://hoploninfosec.com/hospital-clinic-was-under-ransomware-attack

[59] Associated Press, “Cyberattack Hits Major Hospital in Spanish City of Barcelona”, (2023). Retrieved from: https://www.securityweek.com/cyberattack-hits-major-hospital-in-spanish-city-of-barcelona/

[60] CERT-EU, “Cyber Security Brief 23-04 - March 2023”, (2023). Retrieved from: https://cert.europa.eu/publications/threat-intelligence/cb23-04/

[61] Higuera, A., “El ciberataque al Clínic una semana después: un grupo internacional acusado, 4 terabytes de datos robados y un hospital paralizado”, (2023). Retrieved from: https://www.20minutos.es/tecnologia/ciberseguridad/el-ciberataque-al-clinic-una-semana-despues-un-grupo-internacional-acusado-4-terabytes-de-datos-robados-y-un-hospital-paralizado-5109043/

[62] INCIBE-CERT, “Ransomware cyberattack paralyses activity at Hospital Clínic in Barcelona”, (2023). Retrieved from: https://www.incibe.es/en/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-ransomware-paraliza-actividad-del-hospital

[63] Clínic Barcelona(b), “Statement on the computer attack on the FRCB-IDIBAPS 15/05/2023”, (2023), Retrieved from: https://www.clinicbarcelona.org/en/news/computer-attack-on-the-frcb-idibaps

[64] Clínic Barcelona(c), “Statement on the computer attack on the FRCB-IDIBAPS 15/07/2023”, (2023), Retrieved from: https://www.clinicbarcelona.org/en/news/computer-attack-on-the-frcb-idibaps

[65] Government of Catalonia, “Comunicat de premsa sobre el ciberatac a l'Hospital Clínic de Barcelona”, (2023). Retrieved from: https://govern.cat/salapremsa/notes-premsa/490222/comunicat-premsa-sobre-ciberatac-lhospital-clinic-barcelona

[66] France Travail, “France Travail et Cap emploi victimes d'une cyberattaque”, (2024). Retrieved from: https://www.francetravail.org/accueil/communiques/2024/france-travail-et-cap-emploi-victimes-dune-cyberattaque.html?type=article

[67] Commission Nationale de l'Informatique et des Libertés, "Data breach: FRANCE TRAVAIL fined €5 million", (2026). Retrieved from: https://www.cnil.fr/en/data-breach-5million-fine-france-travail

[68] Jones, C., "Record breach of French government exposes up to 43 million people's data", (2024). Retrieved from: https://www.theregister.com/2024/03/14/mega_data_breach_at_french/

[69] Poireault, K., "French Employment Agency Data Breach Could Affect 43 Million People", (2024). Retrieved from: https://www.infosecurity-magazine.com/news/french-employment-agency-data/

[70] Agence France Presse, "France Arrests Three For Theft Of 43 Million Jobseeker File", (2024). Retrieved from: https://www.barrons.com/news/france-arrests-three-for-theft-of-43-million-jobseeker-files-a26d540a

[71] Le Monde, "Cyberattaque de France Travail : les données de 43 millions de personnes « ont potentiellement été exfiltrées »", (2024). Retrieved from: https://www.lemonde.fr/pixels/article/2024/03/13/france-travail-victime-d-une-cyberattaque-les-donnees-de-43-millions-de-personnes-menacees_6221831_4408996.html

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[11]

I, Priscila da Silva Leopoldino

1 grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "[Thesis title]" , supervised by [Supervisor's name]

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2 I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3 I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[11] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Shortlisted cyber-attacks

#	EuRepoC ID	Cyber-attack summary	Start date	Affected member state(s)	Target type	Incident type (EuRopeC)	External threat to EU and its member states? (Y/N)	Regulation (EU) 2016/796 Article 2 proxy
1	1873	Wizard Spider targeted Irish Health Service Executive (HSE)	14.05.2020	Ireland	Critical infrastructure	Data theft & doxing; disruption; ransomware	Y	a, b, d, e, f, g
2	2020	Ransomware attack on Hospital Clinic Barcelona	02.03.2023	Spain	Critical infrastructure	Disruption, ransomware	Y?	a, d, e
3	2218	Medusa ransomware targeted Italian water supplier Alto Calore	01.04.2023	Italy	Critical infrastructure	Data theft; disruption; ransomware	Y?	a, d, e, f
4	3265	French governmental employment agencies targeted, large data theft	06.02.2024	France	State institutions	Data theft, hijacking	Y?	b, f, g
5	1824	LockBit ransomware attack on Portuguese hospital	25.12.2022	Portugal	Critical infrastructure	Data theft; disruption; ransomware	Y	(a,d,e,f,g)
6	2675	Rhysida disrupted Portuguese administration services	27.09.2023	Portugal	State institutions	Data theft; disruption; ransomware	Y?	(a,d,e,f,g)
7	3150	Blackout ransomware attack on French hospital	11.02.2023	France	Critical infrastructure	Data theft; disruption; ransomware	Y?	(a,d,e,f,g)
8	3594	LockBit attacked Croatian University Hospital Centre	27.06.2024	Croatia	Critical infrastructure	Data theft; disruption; ransomware	Y	(a,d,e,f,g)
9	4235	LockBit partially encrypted/exfiltrated data from German schools	14.01.2025	Germany	Critical infrastructure / state	Data theft; disruption; ransomware	Y	(a,d,e,f)
10	4473	EuroCert breach exposed identity docs and prosecutors, Poland	12.01.2025	Poland	Critical infrastructure / state	Data theft; disruption; ransomware	Y?	(a,d,e,f,g)

Figure 1: Shortlisted cyber-attacks.

Appendix 3 – Mapping selected cyber-attacks characteristics against Article 2 of Regulation (EU) 2019/796

Case study: Health Service Executive 2021 ransomware attack

Table 2: Health Service Executive case study against Article 2 criteria.

Article 2 criteria	Assessment	Key evidence
Article 2(a): scope, scale, impact or severity of disruption	Plausibly satisfied	Nationwide health IT disruptions, clinical systems disrupted, fallback to manual operations; approximately 80% of IT systems encrypted [38].
Article 2(b): the number of natural or legal persons, entities or bodies affected	Plausibly satisfied	HSE nationwide infrastructure; approximately 4,000 locations and 54 hospitals affected; 113,00 individuals notified concerning data breach [38], [45].
Article 2(c): the number of member states concerned	Partially satisfied	The cyber-attack was confined to Ireland.
Article 2(d): the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property	Plausibly satisfied	Immediate costs of approximately €102 million; the Comptroller and Auditor General reported €37 million in revenue expenditure and €14 million in capital expenditure in 2021 directly associated with the attack, plus €4.4 million in 2022; projected cyber resilience investment estimated at €657 million over seven years; ongoing litigation led to additional uncertain

		financial loss [39], [49], [51], [53], [54].
Article 2(e): the economic benefit gained by the perpetrator, for himself or for others	Partially satisfied	Ransom of approximately $20 million was demanded by the attackers; HSE refused to pay and attackers later released the decryption key; no publicly available evidence confirming financial gains from the cyber-attack [39], [40], [41].
Article 2(f): the amount or nature of data stolen or the scale of data breaches	Plausibly satisfied	Unauthorised access or copying of personal, financial, medical, and internal administrative data; approximately 113,000 individuals were notified in connection to the breach [43], [44], [45].
Article 2(g): the nature of commercially sensitive data accessed	Partially satisfied	Public reporting indicates access to internal administrative data and employee financial records; the evidence primarily emphasises exposure of personal and medical data than commercially sensitive information [43], [44].

Case study: Hospital Clínic de Barcelona 2023 ransomware attack

Table 3: Hospital Clínic de Barcelona case study against Article 2 criteria.

Article 2 criteria	Assessment	Key evidence

Article 2(a): scope, scale, impact or severity of disruption	Plausibly satisfied	The ransomware disrupted HCB's IT systems, forcing manual workarounds and leading to cancellation of 450 surgeries, 11,000 outpatient visits, and 4,000 laboratory analysis [57], [58], [60] [61].
Article 2(b): the number of natural or legal persons, entities or bodies affected	Plausibly satisfied	Large number of patients affected as a consequence cancelled medical procedures and consultations [57], [58], [61].
Article 2(c): the number of member states concerned	Partially satisfied	The cyber-attack was confined to Spain.
Article 2(d): the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property	Partially satisfied	Cancellation of surgeries and medical consultations; operational disruption of HCB services [57], [58], [60], [61].
Article 2(e): the economic benefit gained by the perpetrator, for himself or for others	Partially satisfied	Ransom demand of $4.5 million issued but not paid [61], [62].
Article 2(f): the amount or nature of data stolen or the scale of data breaches	Plausibly satisfied	Personal data of HCB staff and biomedical research patients exfiltrated and published on the dark web [63], [64].
Article 2(g): the nature of commercially sensitive data accessed	Not satisfied	No evidence that proprietary or commercially sensitive institutional data was accessed.

Case study: France Travail 2024 data breach

Table 4: France Travail case study against Article 2 criteria.

Article 2 criteria	**Assessment**	**Key evidence**
Article 2(a): scope, scale, impact or severity of disruption	Partially satisfied	Large-scale data breach affecting 43 million individuals; no evidence of service disruption [66], [67], [68], [69], [71].
Article 2(b): the number of natural or legal persons, entities or bodies affected	Plausibly satisfied	43 million individuals potentially affected [66], [67].
Article 2(c): the number of member states concerned	Partially satisfied	Cyber-attack contained to France; no cross-border impact.
Article 2(d): the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property	Not satisfied	No quantified economic loss; €5 million CNIL fine reflects regulatory scrutiny, not direct economic loss [67].
Article 2(e): the economic benefit gained by the perpetrator, for himself or for others	Not satisfied	No publicly available evidence of ransom or financial gain.
Article 2(f): the amount or nature of data stolen or the scale of data breaches	Plausibly satisfied	Personal data including names, dates of birth, social security numbers, and contact information [66], [67].
Article 2(g): the nature of commercially sensitive data accessed	Not satisfied	No publicly available evidence of commercially sensitive or strategic data accessed.