Int. Cybersecur. Law Rev. (2022) 3:51–114
https://doi.org/10.1365/s43439-021-00044-5

European Cybersecurity Certification Schemes and cybersecurity in the EU internal market

Donald David Stewart Ferguson

Received: 26 September 2021 / Accepted: 9 December 2021 / Published online: 28 January 2022

Abstract The principal question addressed by this paper is: how adequate are the minimum security objectives of the European Union Cybersecurity Act (Regulation (EU) 2019/881) in assisting organisations in the European Union internal market with resisting and recovering from cyber threats? The question is answered by first identifying the scope of the minimum security objectives. Scope identification, performed through legislative interpretation, reveals an integrated system of security objectives with significant gaps. Second, the minimum security objectives are evaluated within a model of cyber attacks from attack reconnaissance to legal proceedings to reveal further significant gaps. Finally, the minimum security objectives are evaluated within five cyber attack scenarios, reflecting the highest ranking cyber threats to the internal market. The simulation analysis accentuates the findings of the model analysis and identifies further significant gaps. In conclusion, the minimum security objectives are found to be largely inadequate in assisting organisations in the European Union internal market with resisting and recovering from cyber threats. The analysis of the adequacy of the minimum security objectives is timely, as the first European cybersecurity certification schemes are currently being designed.

Keywords European Union Cybersecurity Act · Cyber attack · Cyber kill chain · Advanced persistent threat actor

Donald David Stewart Ferguson
Visiting research fellow at Masaryk University, Brno, Czech Republic

University of Göttingen, Niedersachsen, Germany
E-Mail: donald.ferguson@stud.uni-goettingen.de

1 Introduction

1.1 Background

The Cybersecurity Act is a recent piece of European Union ('EU') legislation directed at improving the functioning of the EU internal market by increasing the level of cybersecurity in the EU internal market [1, Arts. 1(1)(b), 46(1), recs. 1–3, 5]. The Cybersecurity Act seeks to do this by providing a framework for European cybersecurity certification schemes ('ECCS's), *inter alia* [1, Art. 1(1)]. ECCSs identify an adequate level of cybersecurity for information and communications technology ('ICT') products, services or processes ('PSP's) in the EU internal market, but do not ensure that ICT PSPs are completely secure [1, Arts. 1(1)(b), 46(2), 56(3), 67(2), recs. 7, 77].

1.2 Principle question

A principal question is: how adequate is the level of cybersecurity identified by ECCSs for the functioning of the EU internal market? The level of cybersecurity identified by ECCSs is challenging to assess as there are no ECCSs publicly available [1, Art. 49, 2–4]. The minimum level of cybersecurity identified by ECCSs may, however, be found in the minimum security objectives of ECCSs, as specified in Article 51 of the Cybersecurity Act [1]. The ability of these objectives to impact the functioning of the EU internal market includes their ability to assist organisations in the EU internal market with resisting and recovering from cyber threats. The principal question may be re-phrased as: how adequate are the minimum security objectives in Article 51 of the Cybersecurity Act in assisting organisations in the EU internal market with resisting and recovering from cyber threats?

1.3 Methodology

The question of adequacy here is a question of efficacy. The efficacy of legislation can be assessed in a variety of ways, including: the degree of compliance with the legislation, how the legislation affects behaviour, how the legislation is implemented, how the legislation is enforced and how legislation leads to intended real world outcomes [5–7, pp. 1–3]. The principal question is most consistent with outcome assessment, as it focuses on how the minimum security objectives protect organisations against real world cyber threats.

Outcome assessments may be performed qualitatively or quantitatively [8, pp. 9–16]. The Cybersecurity Act does not provide performance indicators for quantitative outcome assessment [1, Art. 67(2), rec. 5]. Furthermore, in the absence of publicly available ECCSs, there are no specific security features of ICT PSPs on which to base quantification [1, Art. 49(7), 2, 3]. The outcome assessment will be performed qualitatively. The qualitative analysis will focus on modelling and simulation of prospective incidents, rather than on case studies of past incidents, as in the absence of publicly available ECCSs, there are no past incidents involving ECCSs to assess.

The analysis will proceed in three stages. First, the scope of ICT PSPs and the minimum security objectives will be identified and clarified to support outcome analysis. Second, outcome analysis of the minimum security objectives will be performed using a model of cyber attacks. Third, outcome analysis of the minimum security objectives will be performed using simulated real world cyber threats that represent the main cyber threats facing the EU internal market. The ability of organisations in the EU to recover from cyber threats includes legal action following a cyber incident, and as a result the model and simulation analyses will also consider how the minimum security objectives in Article 51 of the Cybersecurity Act impact the availability of evidence, as well as the admissibility of evidence in legal action following a cyber incident.

2 Scope identification and clarification

2.1 Methodology

The ICT PSPs and minimum security objectives will be identified individually on the basis of their description in the Cybersecurity Act. The scope of each ICT PSP and minimum security objective will then be clarified through individual legislative interpretation and integration analysis. Integration analysis will consider how each ICT PSP and minimum security objective integrates with each other, on the basis of their individual legislative interpretations. Legislative interpretation will consider the literal, systematic, functional, purposive and consequentialist perspectives on legislative interpretation, where applicable [9, p. 537, 10, p. 979, 11, pp. 13–14, 16, 22, 24–27].[1] The historical approach to legislative interpretation will not be used, as there is insufficient direct causal linkage between the legislative provisions in question and what motivated their specific content and approval [9, pp. 553–555, 10, p. 979, 11, pp. 19–24, 12–14].[2] The focus of clarification will be on what directly impacts the model and simulation outcome analyses performed, as that is the focus of the work.

[1] Literal interpretation of legislation focuses on the usual meaning of the words [1, p. 550, 1, p. 6]. Systematic interpretation focuses on avoiding conflict and duplication between legislative provisions that are part of the same legislative scheme [1, p. 552, 1, pp. 13–14]. Functional interpretation focuses on preserving the effectiveness, or '*effet utile*', of the legislation [1, p. 555, 1, p. 25]. Purposive interpretation focuses on the consistency of legislative interpretation with the purpose of the legislation [1, p. 555, 1, p. 25]. Consequentialist interpretation, finally, focuses on the likely functional consequences of a particular interpretation of legislative provisions [1, p. 555, 1, p. 25].

[2] Historical interpretation focuses on the intent of the legislators as established through evaluation of documentation of the legislative process [1, pp. 553–555, 1, pp. 19–24].

2.2 ICT PSPs

2.2.1 ICT products

ICT products are defined in the Cybersecurity Act as 'an element or group of elements of a network or information system' [1, Art. 2(12)]. The phrase 'network or information system' is not defined in the Cybersecurity Act, but 'network and information system' is defined in the Cybersecurity Act by reference to the NIS Directive [1, Art. 2(2), 15]. The use of the disjunctive 'or', rather than a conjunctive 'and' in the definition of ICT products is the only such disjunctive construction of the terms 'network' and 'information system' in the Cybersecurity Act, Network and Information Systems (NIS) Directive or NIS Implementing Regulation [1, 15, 16]. This implies legislative intent to provide a different meaning.

A 'network and information system' is defined in the NIS Directive as: 'an electronic communications network' as defined in the Framework Directive (2002) [17, Art. 2(a)]; 'any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data'; or 'digital data stored, processed, retrieved or transmitted by elements covered under the above for the purposes of their operation, use, protection and maintenance' [15, Arts. 4(1)(a)-(c)]. Basically, a 'network and information system' refers to three components: an electronic communications network, devices that automatically process digital data pursuant to a program or digital data used by such networks and devices.

On literal interpretation, a 'network or information system' refers to either a 'network' or an 'information system'. On systematic interpretation, an electronic communications network as defined in the NIS Directive would likely be considered a type of 'network' [15, Art. 4(1)(a), 17, Art. 2(a)]. Similarly, on systematic interpretation, a device or group of devices that automatically process digital data pursuant to a program as defined in the NIS Directive would likely be considered a type of 'information system' [15, Art. 4(1)(b)]. This is consistent with the definition of an 'information system' under the Attacks Against Information Systems Directive [18, Art. 2(a)]. As such, an ICT product is at least an element of a 'network and information system'. This is consistent with purposive interpretation, as the purpose of the ECCS framework is to protect network and information systems [1, Arts. 1(1)(b), 2(1)-(2), 2(8), 46(1)].

One clarification is required in interpreting an ICT product as at least an element of a 'network and information system'. Digital data is a component of a 'network and information system', separated in its definition from the other components by a disjunctive 'or' [15, Arts. 4(1)(a)-(c)]. A question arises as to whether digital data on its own can be an ICT product. On literal interpretation, digital data is a component of a 'network and information system', but only to the extent that it is stored, processed, retrieved or transmitted by elements of electronic communication networks or devices for their operation, use, protection and maintenance. The necessary conjunction between digital data and the network or device it is associated with implies mutual dependency. As such, an ICT product will be considered an element of either: a network, including its digital data, or a device, including its digital data, but not digital data alone.

2.2.2 ICT services

ICT services are defined in the Cybersecurity Act as consisting 'fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems' [1, Arts. 2(2), 2(13)].

Integration analysis reveals a dependency between ICT products and ICT services. As ICT products are an element of a 'network and information system', ICT services may transmit, store, retrieve or process information by means of ICT products. One consequence is that ICT services may fulfil the minimum security objectives through the use of ICT products, which may, or may not, independently fulfil the minimum security objectives.

On broader integration analysis, ICT services likely include information society services, such as digital service providers under the NIS Directive [15, Arts. 4(5)-(6)]. ICT services and information society services are both provided by electronic means; yet information society services are circumscribed by the requirements of: provision at a distance, remuneration (direct or indirect) and individual request [15, Arts. 4(1)(a)-(c), 19, para. 110, 20, para. 113, 21, paras. 26–30, 22, Art. 1(1)(b), 23, paras. 34–43, 24, paras. 33–40, 25, paras. 18–27]. The correlation with digital service providers under the NIS Directive is important, as ECCSs are to contribute to implementation of the NIS Directive, starting with cloud service providers [1, Art. 56(3), recs. 65, 92, 2, 3].

2.2.3 ICT processes

ICT processes are defined in the Cybersecurity Act as 'activities performed to design, develop, deliver or maintain an ICT product or ICT service' [1, Art. 2(14)].

On integration analysis, ICT products and services may not be fully functional or operational during design, development, delivery or maintenance, requiring their minimum security objectives to be met by ICT processes during those activities. A deeper dependency exists in that ICT processes may use ICT products and services, including in meeting the minimum security objectives. Those ICT products and services may, or may not, independently meet the minimum security objectives. The provision of security external to ICT PSPs in each case—ICT processes for ICT products and services, and ICT products and services for ICT processes—can impact supply chain risk exposure and allow ICT PSPs that specialise in security to be involved [26–29].

2.3 Minimum security objectives

The minimum security objectives that ECCSs are to achieve may be categorised as: data protection, access limitation, usage logging, restorability, security by design, security by default, vulnerability and dependency identification, as well as secure updates [1, Arts. 51(a)-(j)].

2.3.1 Data protection

Data protection refers to protection of stored, transmitted or otherwise processed data from accidental or unauthorised: access, storage, processing, disclosure, destruction, loss, alteration or lack of availability during the entire life cycle of ICT PSPs [1, Arts. 51(a)-(b)].[3]

The object of protection in data protection is not simply data, but rather: stored data, transmitted data or what is referred to as 'otherwise processed data' [1, Arts. 51(a)-(b)]. The refinement appears intentional, but neither type of data is defined in the Cybersecurity Act [1, Arts. 2(1)-(22)]. The scope of 'otherwise processed data' is particularly vague. On literal interpretation, the phrase 'stored, transmitted or otherwise processed data' implies that processed data includes stored and transmitted data [1, Arts. 51(a)-(b)]. That is not completely supported by systematic interpretation. Processed data appears to be separate from stored and transmitted data in other parts of the Cybersecurity Act, as well as in the NIS Directive [1, Arts. 2(13), 46(2), 51(a), rec. 75, 13, Arts. 4(1)(c), 4(2), rec. 46]. In the General Data Protection Regulation (GDPR), however, storage and transmission are part of processing of personal data [30, Arts. 4(2), 4(12), 31, p. 72, 32, pp. 9–12]. In light of the clarity of the literal interpretation and divergence in systematic interpretation, the literal interpretation that processed data includes stored and transmitted data is preferred [11, p. 7].

The scope of 'otherwise processed data' may be further clarified by systematic interpretation extending to the usage logging minimum security objectives [1, Arts. 51(e)-(f)]. The usage logging objectives require ICT PSPs to record and make it possible to check which ICT PSP data, services or functions have been accessed, used or otherwise processed, at what times and by whom [1, Arts. 51(e)-(f)]. Literal interpretation of the phrase 'accessed, used or otherwise processed' in relation to data implies that processed data includes accessed and used data. This is consistent with systemic interpretation that extends to the GDPR, where processing of personal data includes retrieval and use of personal data [30, Arts. 4(2), 4(12), 31, p. 72, 32, pp. 9–12]. This is, however, not consistent with one clause in a data protection minimum security objective where processing of data and access to data are separated by a disjunctive 'or'; however, the guiding force of that clause for exclusive interpretation may be limited, as it includes stored data in the same list of terms, and stored data is explicitly part of processed data within data protection [1, Arts. 51(a)-(b)]. In light of the clarity of the literal interpretation, it will be preferred, such that processed data includes at least transmitted, stored, accessed and used data [1, Arts. 51(a)-(b), (e)-(f), 11, p. 7].

The duration of data protection is the 'life cycle' of the ICT PSP [1, Arts. 51(a)-(b)]. The 'life cycle' of ICT PSPs is not defined in the Cybersecurity Act [1, Arts. 2(1)-(22)]. On literal interpretation, a 'life cycle', in analogy to a human

[3] This is broader than the scope of data protection under the GDPR, as the GDPR addresses only personal data (not all processed data), but is also narrower in another regard, as the GDPR extends not just to protection of personal data, but also the processes around processing of personal data [30, Arts. 1(1), 2(1), 4(1)-(2), 32, 31, pp. 55–59, 72, 74–75, 187–188, 32, pp. 9–23, 33, pp. 114–115].

life cycle, may refer to the stages from conception to development, maturity, end of life and disposal. This is mirrored to an extent by systematic interpretation extending to ICT processes, which include the design (conception), development, delivery and maintenance (during maturity) of ICT products and services [1, Art. 2(14)]. The life cycle of an ICT PSP may therefore include design, development, delivery, maintenance, end of life and disposal. Further clarity through systematic interpretation is limited by the fact that the term 'life cycle' is not present in the NIS Directive, Regulation on elecronic identification and trust services (eIDAS), Framework Directive (2009), European Electronic Communications Code or GDPR [15, 30, 34–36]. The term 'life cycle' is present in the NIS Implementing Regulation, but with no further clarification on what a 'life cycle' includes [16, Art. 2(1)(a)].

Observing data protection as a whole, data protection uses disjunctive construction of the objects of data protection through use of the word 'or'. Data protection is constructed as: protection of stored, transmitted or otherwise processed data from accidental or unauthorised: access, storage, processing or disclosure; and as protection of stored, transmitted or otherwise processed data from accidental or unauthorised: destruction, loss, alteration or lack of availability [1, Arts. 51(a)-(b)]. Regardless of whether the disjunctive construction is inclusive or exclusive, on literal interpretation, it narrows the scope of data protection. For example, stored data need only be protected from accidental storage and destruction for the data protection objectives to be met, with no protection of stored, transmitted or otherwise processed data against accidental or unauthorised: access, processing, disclosure, loss, alteration or lack of availability [1, Arts. 51(a)-(b)]. When read in light of recital 75 of the Cybersecurity Act, however, the disjunctive construction may represent accommodation for the fact that not all ICT PSPs may deal with all types of processed data or all types of protected activities with processed data [1, rec. 75]. This favours contextual conjunctive construction, such that the objects of data protection apply fully, to the extent possible for the specific ICT PSP, supporting the *effet utile* of data protection [11, p. 26].

On integration analysis, it is apparent that data protection of an ICT PSP during design and development may need to be performed external to the ICT PSP. This is because data protection functionality may not be complete until the design and development of the components of the ICT PSP requiring data protection are complete.[4] Furthermore, data protection of an ICT PSP may need to be supplemented by measures external to the ICT PSP during delivery, maintenance, end of life and disposal, as the ICT PSP may not be fully functional during those stages.[5] ICT processes may provide external data protection for ICT products and services during at least design, development, delivery and maintenance; however, protection during end of life and disposal, as well as protection of ICT processes themselves through their life cycle, may require other measures [1, Art. 2(14)]. The benefits of external security, as indicated previously for ICT processes, apply, but are offset

[4] Particularly at the early stages of design and development, and through design and development until testing is complete.

[5] This is particularly important as it represents stages of the life cycle of an ICT PSP where the ICT PSP is exposed outside of the control of the ICT PSP provider.

where the ICT PSPs providing that external security do not independently meet the minimum security objectives.

2.3.2 Access limitation

Access limitation means that authorised persons, programs or machines are only able to access data, services or functions to which their access rights refer [1, Art. 51(c)]. Neither determinative term is defined in the Cybersecurity Act [1, Arts. 2(1)-(22)]. The disjunctive 'or' construction is also present here, and for similar reasons as for data protection, will be read in a contextual conjunctive manner: to address access by all persons, programs and machines to all data, services and functions that apply to a specific ICT PSP in order to support the *effet util* of access limitation.

On literal interpretation, as the subject of access limitation is authorised persons, programs or machines, access limitation does not extend to unauthorised persons, programs or machines [1, Art. 51(c)]. Consequently, authorised persons would be subject to access limitation, while unauthorised persons would not, undermining the *effect util* of access limitation. On purposive interpretation, as the purpose of ECCSs includes protecting the confidentiality of ICT PSP data, services or functions, that would also include protecting the confidentiality of ICT PSP data, services or functions from unauthorised persons, programs and machines with no access rights [1, Art. 46(2)]. In light of the consequentialist and purposive interpretations, the preferred interpretation is that access limitation extends to limitation of unauthorised persons, programs and machines—with no access rights, from access to ICT PSP data, services and functions [37, paras. 14, 26].

On integration analysis, access limitation likely implements the 'unauthorised' access aspect of data protection [1, Arts. 51(a)-(c)]. Access limitation is broader than data protection, however, in that access limitation addresses unauthorised access to all ICT PSP data, as well as the services and functions of ICT PSPs [1, Arts. 51(a)-(c)]. Data protection is restricted to processed data, but addresses a broader set of activities with processed data than just access, such as: storage, processing, disclosure, destruction, loss, alteration and lack of availability [1, Arts. 51(a)-(b)]. However, the broader set of activities likely require initial access to the processed data, and as such initially fall within the scope of access limitation—except for loss and lack of availability. Adding a dimension, the data that access limitation uses to function, such as authentication data and access right data, likely falls within the scope of data protection as stored data, and as transmitted data where authentication data is transmitted [1, Arts. 51(a)-(b)]. Furthermore, access limitation data, services and functions would likely be protected by access limitation itself in order to give *effet util* to access limitation [1, Art. 51(c), 38, paras. 17, 22(11), 24].

On literal interpretation, access limitation does not explicitly extend throughout the life cycle of ICT PSPs as data protection does [1, Arts. 51(a)-(c)]. On functional interpretation, however, as access limitation likely implements part of data protection, access limitation would have to extend throughout the life cycle of ICT PSPs to give *effet utile* to data protection. Furthermore, on purposive interpretation, as the purpose of ECCSs includes protecting processed data, services and functions of ICT PSPs throughout their life cycle, the protection that access limitation pro-

vides should extend throughout the life cycle of ICT PSPs [1, Art. 46(2)]. Finally, as access limitation may not be fully functional in an ICT PSP during its design, development, delivery, maintenance, end of life or disposal, access limitation would have to be provided external to the ICT PSP in those stages.[6] Again, the benefits of external security, as indicated previously for ICT processes, apply here, but are offset where the ICT PSPs providing that external security do not independently meet the minimum security objectives.

2.3.3 Usage logging

ICT PSPs are required to record and make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom [1, Arts. 51(e)-(f)]. Neither of the determinative terms are defined in the Cybersecurity Act [1, Arts. 2(1)-(22)]. The use of disjunctive 'or' construction is present again, and may be read, for similar reasons as for data protection, in a contextual conjunctive manner to support the *effet utile* of usage logging. The phrase 'otherwise processed' arises here again in relation to data, and for the reasons expressed for data protection, 'processed' data in relation to usage logging includes at least accessed, used, stored and transmitted data [1, Arts. 51(a)-(b), (e)-(f)].

The phrase 'by whom' requires clarification, as on literal interpretation it may extend only to persons [1, Arts. 51(e)-(f)]. On systematic interpretation, as access limitation includes access by persons, programs and machines, access 'by whom' under usage logging may in parallel include access by persons, programs and machines [1, Arts. 51(c), (e)-(f)]. This is supported by functional interpretation, as persons, programs and machines may all access ICT PSPs, and as such extension of 'by whom' to programs and machines may be required to give *effet utile* to usage logging.

On integration analysis, the scope of access limitation and usage logging overlap significantly in their objects of protection: they both address access to data, services and functions of ICT PSPs [1, Arts. 51(c), (e)-(f)]. As usage logging records access to and usage of data, services and functions, it likely records access to and usage of access limitation data, services and functions [1, Arts. 51(c), (e)-(f)]. The inclusion is important as it provides for the ability to record and observe which persons, programs and machines are attempting to access and use access limitation data, services and functions [39, paras. 29–30, 41, 44, 47]. The integration of usage logging and data protection is more complex.

Usage logging addresses all data, services and functions of an ICT PSP, while data protection addresses only processed data [1, Arts. 51(a)-(b), (e)-(f)]. Data protection addresses a broader set of activities than usage logging, extending to: disclosure, destruction, loss, alteration and lack of availability of processed data [1, Arts. 51(a)-(b), (e)-(f)]. However, as disclosure, destruction and alteration of processed data may require access to processed data, and represent use of processed data, they likely fall

[6] A pattern is forming where during many stages of the life cycle of an ICT PSP, the implementation of the minimum security objectives is not expected to be fully functional within the ICT PSP, requiring external measures.

within the scope of usage logging [1, Arts. 51(a)-(b), (e)-(f)]. The overlap between data protection and usage logging is important because it allows usage logging of activities protected by data protection, while concurrently recording data protection services and functions in order to identify how data protection is operating [40, paras. 21, 36(3)].

Considering the integration of usage logging, data protection and access limitation from another perspective, as usage logging creates data that is stored through recording, the data created by usage logging likely falls within the scope of data protection and access limitation, and, consequently, usage logging of each. This provides *effet utile* and fits with purposive interpretation, as the integrity and authenticity of usage logging data would not be reliable unless its modification could be protected and tracked reliably [1, Art. 46(2)].

On broader integration analysis, although usage logging does not provide any direct protection of ICT PSPs, as it merely records activity and allows the activity to be observed, usage logging enables broader ICT PSP protection by notifying organisations of activity with the ICT PSP, so that the organisation can engage other security measures to address that activity [41–48, p. 21, 49–55].

On literal interpretation, usage logging does not explicitly extend throughout the life cycle of ICT PSPs [1, Art. 51(a)-(b), (e)-(f)]. On purposive interpretation, however, as the purpose of ECCSs includes protecting processed data, services and functions of ICT PSPs throughout their life cycle, the ability of usage logging to protect ICT PSPs, such as through linkage to other organisational measures, would need to extend through the life cycle of ICT PSPs [1, Art. 46(2)]. As usage logging may not be fully functional in an ICT PSP during its design, development, delivery, maintenance, end of life or disposal, usage logging would have to be provided external to the ICT PSP in those stages.[7] Again, the benefits of external security, as indicated previously for ICT processes, apply here, but are offset where the ICT PSPs providing external security do not meet the minimum security objectives.

2.3.4 Restorability

Restorability requires ICT PSPs to restore availability and access to data, services and functions in a timely manner in the event of a physical or technical incident [1, Art. 51(h)]. Neither of the determinative terms are defined in the Cybersecurity Act [1, Arts. 2(1)-(22)].

On literal interpretation, restorability applies only to availability and access to data, services and functions [1, Art. 51(h)]. Restorability does not include restoration of other activities, such as: use, storage, processing or alteration [1, Arts. 51(a)-(b), (e)-(f), (h)]. In other words, restorability does not restore the full functionality of an ICT PSP. It is recommended that when ECCSs are designed, restorability extend to the full functionality of the ICT PSP under consideration.

Restoration of availability and access are further qualified by the timeliness of restoration [1, Art. 51(h)]. The timeliness of restoration is important to outcome analysis, as it determines when restoration of availability and access are to be complete.

[7] Considering the linkage to other organisational security measures, this is particularly important.

The Cybersecurity Act provides no explicit guidance on the timeliness of restoration [1]. Clarification of the timeliness of restoration requires first a clarification of the degree of restoration required in that timeframe.

On literal interpretation, the word 'restore' is not qualified by a degree of restoration, implying no limitation on the degree of restoration [1, Art. 51(h)]. Furthermore, the restorability objective has a more conjunctive construction than the aforementioned security objectives, with the use of the word 'and', rather than the use of the word 'or': it is availability and access to all: data, services and functions that is to be restored [1, Art. 51(h)]. This permits a greater degree of restoration. Systematic interpretation is not available to elucidate the degree of restoration, as degrees of restoration are not explicitly elaborated on in the Cybersecurity Act, NIS Directive, NIS Implementing Regulation, eIDAS Regulation, Framework Directive (2009), European Electronic Communications Code or GDPR [1, 15, Arts. 14(2), 16(2), 16, Art. 2(3), 30, Art. 32(1)(c), 31, pp. 187–188, 33, pp. 114–115, 34, Art. 13a(2), 35, Art. 19(1), 36, Art. 40(1)]. Functional interpretation supports full restoration, as any degree of restoration below full restoration may undermine the *effet utile* of the restorability objective. For example, restoration of access to 99% of ICT PSP data may be a substantial target, except where the 1% not restored is the access limitation data necessary to access the rest of the data. The timeliness of restoration will be assessed based on complete restoration of access and availability to ICT PSP data, services and functions.

Turning to the timeframe, the first aspect to consider is when the timeframe starts. On literal interpretation, as restoration addresses availability and access 'in the event of' a physical or technical incident, the timeframe likely starts when incomplete availability or access first occur, during or after such an incident. The end of the timeframe, or deadline for timeliness, may, for similar reasons, be considered to occur when availability or access are first requested from the ICT PSP following incomplete availability or access. This may occur virtually immediately. In summary, timeliness of restoration may require, virtually immediate, complete restoration of availability and access to ICT PSP data, services and functions during or after a physical or technical incident.

One concern with this interpretation is that the ongoing nature of an incident may limit the ability to start restoration. That only applies, however, where restorability is coupled to the effects of the ongoing incident. For example, a mirror server in one location may provide availability and access to data regardless of an ongoing physical incident at the site of another mirror server [56]. Another concern with this interpretation is that it appears to be a high standard for a minimum security objective that applies across all ICT PSPs.[8] The minimum security objectives do not, however, seek to provide a minimum level of security, but rather an adequate and higher level of security, initially to support organisations subject to Member State implementations of the NIS Directive, on whom the internal market depends for complete and virtually immediate availability and access [1, Arts. 1(1)(b), 46(1), 56(3), 67(2), recs. 5, 7, 12, 13, 65, 77, 92, 15, Arts. 14(2), 16(2), rec. 48, 16, Art.

[8] It is important to note here that assurance levels do not play a role as they do not determine the security level, but rather the evaluation level [1, Art. 2(21)].

2(3), rec. 4, 57, p. 24]. Furthermore, virtually immediate and complete restoration is currently a reality for data, services and functions through redundant devices [56, 58–60, p. 12, 61, pp. 99–107]. In particular, cloud services, which are currently the focus of ECCS design by ENISA, can provide rapid restoration timeframes [2, pp. 78, 80–81, 3, 58, 59]. The use of redundant devices may be limited for technical reasons for some ICT PSPs [56, 58, 59]. The timeframe for restoration may therefore be interpreted to be as close to immediate as possible, within the limits of what is technically possible for the specific ICT PSP.[9]

The terms 'physical incident' and 'technical incident' are not defined in the Cybersecurity Act. The term 'incident' is defined in the Cybersecurity Act with reference to the NIS Directive, where it refers to any event having an actual adverse effect on the ability of network and information systems to resist actions that compromise the confidentiality, integrity, authenticity or availability of their processed data or services [1, Art. 2(6), 15, Arts. 4(2), 4(7)]. As such, on literal interpretation, a 'physical incident' may relate to an 'incident' caused by a physical event, and a 'technical incident' may relate to an 'incident' caused by a technical event. Systematic interpretation is limited by the fact that the terms 'physical incident' and 'technical incident' are not elaborated on further in the Cybersecurity Act, NIS Directive, NIS Implementing Regulation, eIDAS Regulation, Framework Directive (2009) or the European Electronic Communications Code [1, 15, 16, 30, Art. 32(1)(c), 31, pp. 187–188, 33, pp. 114–115, 34–36]. The terms are used in the GDPR in a similarly worded provision, but are not further elucidated [30, Art. 32(1)(c), 31, pp. 187–188, 33, pp. 114–115].

The fact that 'incident' was not specified alone in the restorability objective, but was qualified into two types of incidents: 'physical' and 'technical', implies that the distinction is important, and that only such incidents need be restored from. This is a concern, however, as human error is a significant issue in cybersecurity and is not by its nature a technical or physical event [1, recs. 8, 10, 62, 63, paras. 1.6, 4.7.1, 64, pp. 7, 9, 12–13]. It is recommended that incidents arising from events of human error be included in the restorability objective in ECCSs.

On integration analysis, restorability implements part of data protection as restorability addresses access, lack of availability, loss and destruction of processed data within the scope of data protection [1, Arts. 51(a)-(b), (h)]. In addition, as restorability restores availability and access to ICT PSP data, services and functions, this includes availability and access to data protection, access limitation and usage logging data, services and functions [1, Arts. 51(a)-(c), (e)-(f), (h)]. The recommendation that restorability extend to the full functionality of an ICT PSP is particularly important, as it would result in restoration of the full functionality of data protection, access limitation and usage logging. The relationship is reciprocal, as restoration data, or 'images', are likely stored, and as such protected by data protection, as well as access limitation and usage logging when accessed and used [1, Arts. 51(a)-(c), (e)-(f), (h)].

[9] It is appreciated that this is likely a controversial interpretation as it may not be cost effective for certain market segments, and may lead to trade-offs in ICT PSP storage capacity and performance.

On literal interpretation, restorability does not explicitly extend throughout the life cycle of ICT PSPs [1, Arts. 51(a)-(b), (h)]. On functional interpretation, considering that restorability implements part of data protection, and provides for the ongoing availability of data protection services and functions following physical and technical incidents, restorability too would likely have to extend throughout the life cycle of ICT PSPs to give *effet utile* to data protection [1, Arts. 51(a)-(b), (h)]. Furthermore, on purposive interpretation, as the purpose of ECCSs includes protecting processed data, services and functions of ICT PSPs throughout their life cycle, the ability of restorability to protect ICT PSPs should extend through the life cycle of ICT PSPs [1, Art. 46(2)]. As restorability may not be fully functional in an ICT PSP during its design, development, delivery, maintenance, end of life or disposal, restorability would likely have to be provided external to the ICT PSP in those stages.[10] Again, the benefits of external security, as indicated previously for ICT processes, apply, but are offset where the ICT PSPs providing that external security do not meet the minimum security objectives independently.

2.3.5 Security by design

ICT PSPs are required to be secure by design [1, Art. 51(i), recs. 2, 12]. Security by design is not defined in the articles of the Cybersecurity Act, but is described in recital 12 as: 'measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyber attacks is presumed and their impact is anticipated and minimized' [1, Arts. 2(1)-(22), rec. 12]. Furthermore, security by design should 'constantly evolve to reduce the risk of harm from malicious exploitation' [1, Arts. 2(1)-(22), rec. 12].

Literal interpretation of the phrase 'measures at the earliest stages of design and development' implies that security by design need occur only at the earliest stages of design and development [1, Arts. 2(1)-(22), rec. 12]. On functional interpretation, however, in order for security by design to have *effet utile*, it would have to exist throughout design and development, as services and functions designed and developed at the end of those stages would also require security measures. As recital 12 is merely guiding, and not binding, security by design is interpreted to extend from the earliest stages of design and development to all stages of design and development of ICT PSPs.

Literal interpretation of the phrase 'highest degree possible' implies that security by design is to provide security measures to the highest possible degree of security attainable. That is not consistent with systematic interpretation, where security measures need only be designed to meet the security requirements of the applicable ECCS [1, Arts. 46(2), 53(2), 56(1)]. As recital 12 is guiding, and not binding, security by design shall be interpreted to refer to protection at least to the degree specified by the applicable ECCS.

[10] This is likely less of an issue during design, development, delivery and disposal, but is particularly important during maintenance, where restorability is a last resort to address issues that arise during, or as a result of maintenance.

On literal interpretation, security by design under recital 12 appears to be limited to protection from cyber attacks [1, rec. 12]. This is not consistent with systematic interpretation, as the other security objectives, which would be expected to be designed through security by design, are not limited to cyber attacks [1, Arts. 51(a)-(j)]. Consequently, should the other objectives be implemented to address other cyber threats without security by design, it would undermine the *effet utile* of security by design, and likely the other security objectives. The purpose of ECCSs is not limited to protecting ICT PSPs from cyber attacks, and as such, limiting security by design to cyber attacks is not consistent with purposive interpretation [1, Art. 46(2)]. Again, as recital 12 is only guiding, security by design is interpreted to address all cyber threats within the scope of ECCSs.

Finally, the impact of cyber attacks is to be anticipated and minimized by security by design [1, rec. 12]. On literal interpretation this is vague, as identification of who is potentially impacted and the threshold of minimisation are not specified. On systematic interpretation, as ECCSs likely already incorporate such an analysis, measures designed to meet the other security requirements of an ECCS likely anticipate and minimise the impact of cyber threats sufficiently from the perspective of the Cybersecurity Act.

On integration analysis, it is implicit that security by design provides the design of the other security objectives. As each security objective clarified to this point requires security external to the ICT PSP during certain stages of the ICT PSP life cycle, security by design would also need to extend to those external forms of protection.

2.3.6 Security by default

ICT PSPs are required to be secure by default [1, Art. 51(i), recs. 13, 87]. Security by default is not defined in the articles of the Cybersecurity Act, but is described in recital 13 [1, Arts. 2(1)-(22), rec. 13]. Security by default requires designers of ICT PSPs to configure their ICT PSPs for a 'higher level of security', so that the first user of the ICT PSP receives 'a default configuration with the most secure settings possible' [1, recs. 13, 87]. Security by default should not require extensive configuration, specific technical understanding or non-intuitive behaviour from the user, should work easily and reliably when implemented and should prompt users for the most secure settings where default settings are not feasible, on the basis of risk and usability analysis [1, rec. 13].

Literal interpretation of the phrases 'higher level of security' and 'most secure settings possible' should be tempered by systematic interpretation such that they refer not to levels of security that may exist beyond those required by an ECCS, but rather represent at least levels of security specified by an ECCS [1, Arts. 46(2), 52, 53(2), 56(1)]. On literal interpretation the same phrases imply that ICT PSPs may also be configured for lower levels of security. On systematic interpretation, however, configuration should not allow the level of security of an ICT PSP to go below the level required by the applicable ECCS, as that would enable a certified ICT PSP to operate as a non-certified ICT PSP, undermining the clarity and confidence

that certification seeks to attain [1, Arts. 1(1), 46(2), 52, 53(2), 56(1), recs. 2, 7, 10, 65–66, 69].

On integration analysis, it is implicit that security by default provides the initial configuration for the other security objectives, as specified by security by design, including implementations external to the ICT PSP. That security configuration data, as stored data, would likely be subject to data protection, while access to security configuration data, services and functions would likely be subject to access limitation, usage logging and restorability on the basis of security by design [1, Arts. 51(a)-(c), (e)-(f), (h), (i)]. This is important as it provides for protection, tracking and rapid restoration of an ICT PSP's security configuration.

2.3.7 Vulnerability and dependency identification

Known dependencies and vulnerabilities of ICT PSPs are to be identified and documented, and ICT PSPs are to be verified to not contain known vulnerabilities [1, Arts. 51(d), (g)]. Neither vulnerabilities nor dependencies are defined in the articles of the Cybersecurity Act [1, Arts. 2(1)-(22)]. Dependencies are described in recital 11 as: 'one or more third-party technologies and components such as software modules, libraries or application programming interfaces' used by ICT PSPs [1, rec. 11]. There is no recital description of vulnerabilities.

On literal interpretation, vulnerabilities in an ICT PSP may be viewed broadly. On systematic interpretation, however, vulnerabilities are more narrowly viewed as aspects of an ICT PSP that prevent it from meeting the security requirements of the applicable ECCS [1, Arts. 46(2), 52, 53(2), 56(1)]. On purposive interpretation, however, vulnerabilities may again be viewed more broadly, to include aspects of an ICT PSP that undermine the purpose of ECCSs, including and beyond the specific security requirements of the ECCS [1, Art. 46(2)]. As ICT PSPs need only meet the requirements of an ECCS for certification, the systematic interpretation is preferred [1, Arts. 46(2), 52, 53(2), 56(1), recs. 7, 77].

It is initially difficult to reconcile the requirement that ICT PSPs do not contain known vulnerabilities with the requirement that known vulnerabilities in ICT PSPs be identified and documented [1, Arts. 51(d), (g)]. This may be reconciled through functional interpretation to include each aspect sequentially: known vulnerabilities are to be identified, documented and verified to no longer exist—presumably after they have been fixed. This is consistent with the interpretation of vulnerabilities as deviations from the security requirements of an ECCS, as they are aspects that need to be identified and fixed in order to comply with ECCS requirements [1, Arts. 46(2), 52, 53(2), 56(1)].

On integration analysis, vulnerability and dependency identification do not explicitly extend through the life cycle of ICT PSPs [1, Arts. 51(d), (g)]. Vulnerabilities may, however, be discovered in implementations of the other minimum security objectives that do extend through the life cycle of ICT PSPs.[11] In order to support the *effet util* of those objectives, vulnerability identification would also need to exist

[11] In light of the integrated nature of the minimum security objectives, vulnerabilities in one implementation of a minimum security objective can significantly affect the other minimum security objectives.

throughout the life cycle of ICT PSPs [1, Arts. 46 (2), 51(a)-(b), (d), (g); 65, p. 25]. The same applies to dependencies, which may contribute to implementations of the minimum security objectives that extend throughout the life cycle of ICT PSPs [1, Arts. 51(d), (i), rec. 12]. Where the implementations of the minimum security objectives are external to an ICT PSP, vulnerability and dependency identification would need to extend to those external aspects, including ICT processes. Finally, vulnerability identification would likely inform security by design, leading to fixes applied via secure updates [1, Arts. 51(d), (g), (i)-(j), recs. 2, 11, 12, 13, 87].

2.3.8 Secure updates

ICT PSPs are to be provided with up-to-date software and hardware, containing no publicly known vulnerabilities, by secure update mechanisms [1, Art. 51(j), recs. 87, 96]. Neither determinative term is defined in the Cybersecurity Act [1, Arts. 2(1)-(22)].

Literal interpretation of the phrase 'publicly known vulnerabilities' may imply that software and hardware updates may include vulnerabilities known to the ICT PSP provider, including severe vulnerabilities, as long as they are not known to the public. That is not consistent with systematic interpretation, however, as ICT PSPs are not to contain any vulnerabilities, regardless of publication [1, Art. 51(g)]. It is recommended that when ECCSs are designed, they require secure updates to contain no vulnerabilities known to the ICT PSP provider.

On literal interpretation, a patch to an ICT PSP may not contain publicly known vulnerabilities, but that does not prevent the patch from causing vulnerabilities in the ICT PSP once applied to the ICT PSP [1, Art. 51(j), rec. 96]. On systematic interpretation, however, as ICT PSPs are not to contain known vulnerabilities, patch updates are likely required to not create vulnerabilities in ICT PSPs when they are applied [1, Art. 51(g), rec. 96]. It is recommended that when ECCSs are designed, they explicitly require secure update patches to not create new vulnerabilities in ICT PSPs.

On integration analysis, it is apparent that secure updates provide a mechanism for the delivery stage of ICT processes [1, Art. 2(14)]. In particular, secure updates provide the mechanism for fixes to vulnerabilities in the implementations of the minimum security objectives, including secure updates themselves, to be applied to an ICT PSP. Secure update data, when transmitted and stored, is protected by data protection, while access to secure update data, services and functions is protected by access limitation, usage logging and restorability [1, Arts. 51(a)-(c), (e)-(f), (h), (j)]. Furthermore, secure updates would be designed by security by design, would be subject to vulnerability and dependency identification, and would be available by default through security by default, as they implement a minimum security objective required by ECCSs [1, Arts. 51(d), (g), (i)-(j)].

On literal interpretation, secure updates do not explicitly extend through the life cycle of ICT PSPs [1, Art. 51(j)]. As secure updates provide the mechanism for vulnerability fixes to be applied to implementations of the minimum security objectives that do extend through the life cycle of ICT PSPs, secure updates would need to extend through the life cycle of ICT PSPs to retain the *effet util* of those

objectives [1, Arts. 51(a)-(b), (g)]. During a secure update, an ICT PSP may not be fully functional, and as such data protection, access limitation, usage logging and restorability of the ICT PSP would have to be provided by the secure update mechanism, or external to the ICT PSP. The benefits of external security, as indicated previously for ICT processes, would apply in the latter case, but would be offset where the ICT PSPs providing that external security do not meet the minimum security objectives independently.

2.3.9 Residual integration analysis

A gap has emerged through progressive integration analysis of the minimum security objectives. The minimum security objectives, taken together, are not sufficient to protect the integrity, authenticity and availability of ICT PSP services and functions while they are operating. This is significant as the purpose of ECCSs includes protecting the confidentiality, integrity, authenticity and availability of processed data, services and functions of ICT PSPs throughout their life cycle [1, Art. 46(2)].

Data protection addresses the confidentiality, integrity, authenticity and availability of processed data, but does not extend to the services or functions of an ICT PSP [1, Arts. 51(a)-(b)]. Looking deeper, as ICT PSP services and functions may be based partially on compiled code and configuration data, which are stored data, the confidentiality, integrity, authenticity and availability of ICT PSPs services and functions are partly protected by data protection of the compiled code and configuration data that underlie the services and functions [1, Arts. 51(a)-(b)]. This does not, however, fully protect the integrity, authenticity and availability of ICT PSP services and functions at runtime—while they are operating. Access limitation protects the confidentiality of ICT PSP data, services and functions, including at runtime, but not their integrity, authenticity or availability [1, Art. 51(c)]. Usage logging allows for protection of ICT PSP data, service and function confidentiality, integrity, authenticity and availability at runtime when the usage logging is monitored, but provides no direct protection itself [1, Arts. 51(e)-(f)]. Restorability restores the availability of ICT PSP data, services and functions after physical and technical incidents, including during runtime, but not their confidentiality, integrity or authenticity; and does not protect the confidentiality, integrity, authenticity or availability of ICT PSPs from incidents in the first place [1, Art. 51(h)]. It is recommended that protection of the confidentiality, integrity, authenticity and availability of ICT PSP services and functions be an explicit security objective when ECCSs are designed, particularly considering the use of certified ICT PSPs by operators of essential services in the internal market [1, Art. 56(3), recs. 65, 92].

2.4 Conclusion

The scope of each ICT PSP and each minimum security objective was identified individually and then clarified through legislative interpretation and integration analysis with a focus on outcome efficacy. During identification it was generally observed that the majority of the terms used to describe the minimum security objectives, including those directly related to outcome efficacy, are not defined in the Cyber-

security Act. This broadens the scope for divergent interpretation, undermining the harmonisation objective of ECCSs and potentially impacting the outcome efficacy of ECCSs [1, Arts. 1(1)(b), 46(1), rec. 95]. Clarification by integration analysis reveals a high degree of integration between the objectives, directly relevant to outcome analysis, and is also not explicit in the Cybersecurity Act. This creates further room for divergent assessments of integration that may undermine the harmonisation objective of ECCSs and impact the outcome efficacy of ECCSs [1, Arts. 1(1)(b), 46(1), rec. 95].

Where clarification was not available through legislative interpretation or integration analysis, recommendations were proposed to contribute to outcome efficacy. The specific recommendations were that when ECCSs are designed:

1. Restorability extend to the full functionality of ICT PSPs
2. Restorability extend to human error incidents
3. Secure updates contain no known vulnerabilities
4. Secure updates create no new vulnerabilities in ICT PSPs
5. Protection of the confidentiality, integrity, authenticity and availability of ICT PSP services and functions be an explicit security objective

Finally, it was consistently observed that the minimum security objectives require implementation external to ICT PSPs during stages of the life cycle of ICT PSPs where ICT PSPs are not fully functional. This is a concern where the implementations are provided by ICT PSPs that do not meet the minimum security objectives themselves [15, rec. 52]. This creates a recursive dependency, where certified ICT PSPs providing external security measures may themselves require external security measures, which would need to be provided by certified ICT PSPs, during stages of their life cycles where they are not fully functional. This may represent an inherent weakness in ECCSs that is not readily apparent, and hence may not only limit the outcome efficacy of ECCS-certified ICT PSPs, but also how that outcome efficacy is communicated and interpreted, including by Courts.

3 Cyber threat model analysis

3.1 Methodology

Cyber threat model outcome analysis will be performed in three steps: selecting the cyber threats to model, selecting a model that supports analysis of the outcome efficacy of the minimum security objectives against the selected cyber threats, and using the model to analyse how the minimum security objectives assist organisations in resisting and recovering from the selected cyber threats.

3.2 Threat selection

The Cybersecurity Act does not identify the individual cyber threats the minimum security objectives are to address [1, Arts. 2(8), 51(a)-(j), recs. 3, 5, 6, 8–9]. The

individual cyber threats to be addressed may include those identified in the NIS Cooperation Group cybersecurity incident taxonomy ('CIT') for incidents under the NIS Directive, Framework Directive (2009) and eIDAS Regulation [64, p. 6]. The CIT provides a consistent reference point for threat identification across EU cybersecurity legislation, including the NIS Directive, which ECCSs are to focus on initially [1, Art. 56(3), recs. 65, 92, 2, 3, 64, p. 6].

In the CIT, root causes are identified as either: system failures, natural phenomena, human errors, malicious actions or third party failures [64, p. 9]. Each root cause represents a class of cyber threat. System failures refer to the failure of a part of a system due to internal causes such as hardware failures, software bugs or flaws in procedures [64, pp. 9, 12–13]. Natural phenomena refer to natural events such as storms and floods [64, pp. 9, 12–13]. Human errors relate to incorrect human usage of a network and information system [64, pp. 9, 12–13]. Malicious actions include cyber attacks and physical attacks [64, pp. 9, 12]. Third party failures refer to disruption of a third party service, such as a power cut [64, pp. 9, 12–13]. As the minimum security objectives are not limited in the cyber threats they are to address, aside from restorability, they may have to address each of these classes of cyber threat [1, Arts. 2(8), 51(a)-(j), 16, Art. 2(1)(b)].

The class of cyber threat to be used for model analysis will be selected based on two criteria: the impact of the cyber threat on the internal market, and how extensively the class of cyber threat challenges the minimum security objectives, in line with the focus on outcome efficacy.

The first criteria will be assessed by reference to incident reporting under EU cybersecurity legislation, specifically: Framework Directive (2009) article 13a and eIDAS Regulation article 19 [34, Art. 13a(3), 35, Arts. 19(2)-(3), 66–71]. Aggregated incident reporting under NIS Directive articles 14 and 16 is not publicly available [13, Arts. 10(3), 14(3), 16(3), 20(1)]. Framework Directive (2009) reporting from 2013 to 2018 illustrates that, on aggregate, system failures were most frequently reported, followed by human error, then natural phenomena, and finally malicious actions [66, pp. 11–12, 67, pp. 15–16, 68, pp. 17–18, 69, p. 19, 70, pp. 17–18, 71, p. 9]. Incidents arising from natural phenomena took the most time to resolve, followed by malicious actions, then system failure, and finally human error [66, p. 15, 67, p. 19, 68, p. 23, 69, pp. 22–23, 70, p. 21]. System errors affected the largest number of user connections, followed by human error, then malicious actions, and finally natural phenomena [66, pp. 15–16, 67, p. 19, 68, p. 22, 69, pp. 22, 70, p. 21]. Under eIDAS Regulation reporting from 2016 to 2018, system failures were most frequently reported, followed by third party failures, malicious actions, and finally human error [72, p. 11, 73, p. 12, 74, p. 8].

The reports of incidents described are limited in how they can inform cyber threat class selection. First, they relate to only two aspects of the EU internal market, and different aspects likely have different threat profiles [62, p. 135, 73, pp. 67–68, 75]. Second, reporting was based on incident thresholds, so not all incidents may have been reported [66, p. 4, 67, pp. 9–10, 68, pp. 9–10, 69, pp. 11–12, 70, p. 11, 72, p. 10, 73, p. 10]. Third, some threats may actively avoid detection, such as malicious actions, and may be under-represented. The second criterion for selection will be

preferred: how extensively a class of cyber threat challenges the minimum security objectives.

Each class of cyber threat can extensively challenge the minimum security objectives, but one class focuses specifically on that: malicious actions. Malicious actions involve threat actors actively and intentionally trying to bypass or take advantage of security measures [76, pp. 67–73, 77, pp. 91–98, 78, pp. 116–124]. Natural phenomena, system failures, third party failures and human errors are unintentional and therefore not focused on specifically challenging security measures. Threat actors in malicious actions may be highly motivated, highly capable and devote significant time and resources to malicious actions, while the other threat classes involve less devotion to directly challenging security measures [76, pp. 67–73, 77, pp. 91–98, 78, pp. 116–124]. Within malicious actions, cyber attacks are considered a greater threat than physical attacks, based on ENISA threat landscape reports from 2016 to 2018 [76, p. 7, 77, p. 9, 78, p. 9]. Cyber attacks will therefore be selected for model analysis.

3.3 Model selection

The model will be selected based on four criteria. First, as cyber attacks are to be assessed, the model needs to be able to address the common steps attackers take in cyber attacks. Second, as security measures representing the minimum security objectives are to be assessed in each cyber attack step, the model needs to be able to address cybersecurity measures against each attack step. Third, as qualitative assessment is to be performed, the model must allow for qualitative assessment. Fourth, as security objectives are being assessed, instead of specific security implementations, the model needs to be able to operate without specific attack techniques, procedures or technologies being provided.

A broad array of models has been assessed against the selection criteria [79–82]. The assessment of three common types of models will be described here: attack trees, attack surfaces and cyber kill chains.

Attack trees depict cyber attack steps in the shape of a tree [81, pp. 70–71, 83]. The attack starts at the root of the tree and branches out along potential attack paths [81, pp. 70–71, 83]. Each path has several steps, or nodes, that represent potential or actual steps in the attack [81, pp. 70–71, 83]. The different models of trees vary in how they annotate the nodes and in their connections to further information [81, pp. 70–71, 83]. Attack trees do not meet the selection criteria as they require identification of specific techniques, procedures and technologies to determine the attack paths and inform the annotation of the nodes [81, pp. 70–71, 83].

Attack surfaces tabulate relative cost–benefit values for attackers to access system entry and exit points [84, p. 371]. The cost is based on the effort required by the attacker to access the entry or exit point, while the benefit is based on the damage potential of the attacker using the entry or exit point [84, p. 371]. Attack surfaces do not meet the selection criteria as they require specification of techniques, procedures and technologies to calculate cost–benefit ratios [84, p. 371].

Cyber kill chains are a series of tactical phases in a cyber attack conceived as links in a chain [85]. A cybersecurity measure that stops one phase in the attack

Table 1 Phases of the Lockheed Martin cyber kill chain in sequential order [85, pp. 4–5]

Phase	Attacker actions
Reconnaissance	Identification, selection and research of targets
Weaponisation	Preparing techniques, procedures and tools for the attack
Delivery	Movement of tools to the target system
Exploitation	Exploiting a vulnerability to gain access to the target system
Installation	Steps to maintain a persistent presence at the target system
Command and Control	Manual access to the target system
Actions on objectives	Steps to achieve the objectives of the attack at the target system: collection or disruption of information, or disruption of systems, includes lateral movement from the target system to access other targets and to act on objectives at the other targets

breaks the chain, halting the entire attack [85, p. 2]. Cyber kill chains were designed to model the most challenging and complex cybersecurity threat actors, termed 'advanced persistent threat' ('APT') actors [85, pp. 1–3]. APT actors are characterised by repetitive attacks over long periods of time using advanced technology and techniques [85, pp. 1–3]. As cyber kill chains are designed to address the most challenging and complex threat actors, cyber kill chains allow assessment of cyber attacks that challenge the minimum security objectives the most. Although not all threat actors are APT actors, APT actors are copied by other threat actors, which makes APT actor tactics anticipatory of other threat actor tactics [78, p. 27]. Cyber kill chains meet the selection criteria as they allow qualitative assessment of common cyber attack steps and cybersecurity measures at those attack steps on a tactical level, independent of specific techniques, procedures and technologies [85, pp. 4–6].

The original, and standard, cyber kill chain model is the Lockheed Martin cyber kill chain ('LM-CKC') [85]. The phases of the LM-CKC are depicted in Table 1.

The defender may use a variety of tactics at each phase, including: detection, denial, disruption, degradation, deception and destruction to stop the attack [85, pp. 5–6]. Defensive strategies adopted in the earlier phases, particularly up to exploitation, are more effective at resisting cyber attacks than strategies at and following exploitation [78, p. 117, 81, pp. 70–71, 85, pp. 6–7].

There are a variety of cyber kill chain variations proposed based on the LM-CKC that variably elaborate on individual phases, omit phases, re-order phases or emphasise lateral movement [86–101]. The LM-CKC will be selected as it is the standard cyber kill chain and represents a common ground between the variants [85]. Furthermore, as the standard cyber kill chain and a common ground between variants, the LM-CKC allows for correlation with a wide variety of cybersecurity literature, including via MITRE tactics and techniques [99–101]. An additional benefit of the LM-CKC is that ENISA uses the LM-CKC in threat landscape reports that could have informed the drafting of the Cybersecurity Act [76, pp. 19, 23, 25, 28–29, 32, 36, 39–40, 42, 45, 47, 50, 52, 56, 58, 61, 65, 77, pp. 29, 35, 38, 44, 48, 54, 59, 63, 67, 70, 74, 78, 81, 86, 89, 78, pp. 32, 36, 40, 46, 53, 58, 63, 68, 73, 77, 84, 91, 99, 106, 113, 131].

The LM-CKC was originally designed for cyber attack analysis and requires two adaptations to allow for analysis of the outcome efficacy of cybersecurity legislation.

Table 2 Modified phases of the Lockheed Martin cyber kill chain in sequential order [85, pp. 4–5]

Phase	Attacker actions	Defender actions
Reconnaissance	Identification, selection and research of targets	Identification of attackers and vectors; tracking updates to attack vectors; detection, denial, disruption, degradation, deception and destruction of attacker reconnaissance
Weaponisation	Preparing techniques, procedures and tools for the attack	Implementing techniques, tools and procedures for: detection, denial, disruption, degradation, deception and destruction
Delivery	Movement of tools to the target system	Detection, denial, disruption, degradation, deception and destruction
Exploitation	Exploiting a vulnerability to gain access to the target system	Detection, denial, disruption, degradation, deception and destruction
Installation	Steps to maintain a persistent presence at the target system	Detection, denial, disruption, degradation, deception and destruction
Command and control	Manual access to the target system	Detection, denial, disruption, degradation, deception and destruction
Actions on objectives	Steps to achieve the objectives of the attack at the target system: collection or disruption of information, or disruption of systems; includes lateral movement from the target system to access other targets and to act on objectives at the other targets	Detection, denial, disruption, degradation, deception and destruction
Damage assessment	Assess the gains of the attack	Assess the losses of the attack
Recovery	Reduce negative consequences to themselves	Reduce negative consequences to themselves
Communication	Communicate the attack in a selected forum	Communicate the attack, recovery and losses to internal and external stakeholders, as well as to authorities
Evidence gathering	Limit evidence gathering	Gather evidence for legal proceedings; provide evidence to authorities and plaintiffs for administrative and Court proceedings
Legal proceedings	Avoid litigation; defend litigation	Initiate own legal proceedings to reduce losses or pursue other goals; cooperate in Court proceedings started by authorities; defend Court proceedings against plaintiffs; defend administrative proceedings by authorities

First, the defender tactics are to be expanded beyond the default detect, deny, disrupt, degrade, deceive and destroy to allow for other cybersecurity tactics [88, pp. 8–9]. Second, phases after Action on Objectives leading up to legal proceedings are to be added in order to reflect ICT PSP incident handling and litigation. The phases added are: Damage Assessment, Recovery, Communication, Evidence Gathering

and Legal Proceedings.[12] The modifications to the LM-CKC are depicted in Table 2 [85, pp. 4–5].

3.4 Model analysis

3.4.1 Reconnaissance

Attacker reconnaissance involves identification, selection and research of targets [85, p. 4]. Defender reconnaissance involves identification of potential attackers and attack vectors, tracking published updates on attack vectors, as well as detection and denial of attacker reconnaissance [85, p. 5]. The defender may also disrupt, degrade and destroy attacker reconnaissance, but such tactics may be considered engaging in illegal cyber attacks [18, Arts. 3–8, 102–104]. The defender may engage in deception, but it can be complex to implement and may be less attainable for all organisations across the EU internal market [105]. The analysis at this phase and in subsequent phases will focus on defender detection and denial.

Defender reconnaissance starts with security by design, where a certified ICT PSP provider identifies potential attackers and attack vectors starting early in design and development [1, Art. 51(i), rec. 12]. This includes known dependencies in order to address supply chain issues, including in internal and external security measures [1, Art. 51(d), rec. 11]. Defender reconnaissance continues with the certified ICT PSP provider tracking published updates on attack vectors as part of ongoing security by design and vulnerability identification [1, Arts. 51(d), (i), rec. 11]. Detection and denial of attacker reconnaissance during certified ICT PSP design, development, delivery, maintenance, end of life and disposal occurs through external security measures, including ICT processes, providing access limitation, data protection and usage logging—where the usage logging data is monitored and acted upon [1, Arts. 2(14), 51(a)-(c), (e)-(f), 106, para. 25(1)]. The importance of data protection, access limitation and usage logging extending through the life cycle of an ICT PSP is apparent here. Where the external measures are not certified, they may be the focus of reconnaissance, unlimited by detection or denial through access limitation, data protection or usage logging.

Attacker reconnaissance on a certified ICT PSP during its operation may be detected and denied via access limitation, data protection and usage logging, where the usage logging data is monitored and acted upon [1, Arts. 51(a)-(c), (e)-(f)]. An attacker may, however, perform reconnaissance on copies of certified ICT products that they acquire, as a common consumer would. Reconnaissance on such copies occurs without detection or denial, as it occurs in isolation from both ICT product providers and potential target organisations. Acquisition of specialised ICT products may, however, lead to detection [97, p. 9]. Attacker reconnaissance on isolated copies of ICT products is mirrored by ICT product providers testing their copies to identify vulnerabilities, and potential target organisations performing vulnerability and penetration testing to test their copies [1, Arts. 51(d), (g), 37, paras. 26, 53,

[12] Although presented as individual, linear phases, the appended phases may practically overlap, occur in different orders and involve cyclic iteration.

38, paras. 31(4), 28(7)-(8), 107, paras. 18(a), 38, 108, pp. 32, 60]. The comparison is important, because the discrepancy observed in systematic versus purposive interpretation of vulnerabilities has a significant effect. An ICT PSP provider is only required to test for vulnerabilities that represent deviations from an ECCS, in line with the systematic interpretation, while attackers and potential target organisations will likely test for vulnerabilities that compromise the availability, authenticity, integrity and confidentiality of processed data, services and functions of an ICT PSP in addition to ECCS requirements, consistent with the purposive interpretation [1, Art. 46(2)]. The distinction reflects how ECCSs are not required to provide absolute protection, and likely requires potential target organisations to perform vulnerability and penetration testing to address the distinction for certified ICT PSPs they use [1, Arts. 1(1)(b), 46(2), 56(3), 67(2), recs. 7, 77, 37, paras. 26, 55, 36, paras. 31(4), 28(7)-(8), 107, paras. 18(a), 38, 108, pp. 32, 60].

Where attacker reconnaissance is limited, this limits the information the attacker has to successfully execute the remaining phases of the kill chain against a hardened target like a certified ICT PSP.[13] This can enter into the cost–benefit assessment of the attacker in deciding whether to proceed with an attack, as this limits the techniques, procedures and tools the attacker can prepare during weaponisation, increasing the chances of detection and denial at later phases in the kill chain.[14] The attacker may focus instead on non-certified ICT PSPs used by organisations, as they may be researched with less risk of detection and denial. This is a concern, as should the attacker be able to exploit a vulnerability in a non-certified ICT PSP, they may be able to use the privileges the non-certified ICT PSP runs under to access the certified ICT PSP as a valid user, unlimited by access limitation or data protection [38, paras. 22(3), 24, 31(3), 44, 45, 49–52, 54, 109, paras. 15–16, 28].

The concern is greater where they are able to escalate their user privileges to administrator rights and modify access limitation data, usage logging data and the overall security configuration of the certified ICT PSP [43, 49, 52, 53, 55, 110, p. 165, 111–115].

A parallel concern is where attackers do not seek reconnaissance on the ICT PSPs of a target organisation, but rather on the employees of the target organisation for social engineering-based attacks [116, p. 102, 117, pp. 145–146, 118]. Where the attacker uses certified ICT PSPs at the target organisation for such reconnaissance, access limitation, data protection and usage logging—where it is monitored and acted upon—can provide for detection and denial [1, Arts. 51(a)-(c), (e)-(f)]. Where the attacker uses non-certified ICT PSPs at the target organisation for social engineering reconnaissance, no such detection or denial may be available. This is important because social engineering may enable the attacker to access certified ICT PSPs in the organisation using valid user rights, unlimited by access limitation, data protection or usage logging [117, pp. 145–146].

[13] This is of central importance for the defender, as will become more apparent through model and simulation analysis.

[14] Attackers adapt to this by developing tools to facilitate reconnaissance within target organisations during the attack.

Once an attacker identifies a vulnerability in a certified ICT PSP, they may spread that knowledge within attacker communities, facilitating reconnaissance by other attackers [49, p. 15, 57, pp. 13–16, 119, 120]. A certified ICT PSP provider that identifies a vulnerability through reconnaissance may publicly provide a fix through secure updates, which may inform attackers about the vulnerability and allow them to use the vulnerability against organisations that are slow to check for and apply updates [38, paras. 22(1)-(2), 24, 121, paras. 35(7)(iii), 37, 47]. An organisation that identifies a vulnerability in a certified ICT PSP during reconnaissance is not required to communicate that vulnerability to other organisations or to the ICT PSP provider, potentially leaving it open for attackers to identify the vulnerability in their reconnaissance [1].

The public availability of ECCS security requirements and ICT PSP provider security usage details supports attacker reconnaissance [1, Arts. 50, 52(3)-(4), 54(1), 55, recs. 85, 93, 122]. ICT PSPs need only meet the minimum security requirements of ECCSs for certification, so there may be less motivation for certified ICT PSP providers to provide security beyond that.[15] The result is that the public availability of ECCSs provides a high level blueprint of the security of certified ICT PSPs across the EU internal market, including those used by operators of essential services subject to national implementations of the NIS Directive, while public availability of ICT PSP provider security usage documentation provides the recommended and hence likely common usage of the security features [1, Art. 56(3), recs. 65, 92].

In summary, the outcome efficacy of the minimum security objectives in detecting and denying attacker reconnaissance is limited by the use of non-certified ICT PSPs connected to certified ICT PSPs, as well as the public availability of: ECCS security requirements, ICT PSP provider security usage details and commercial copies of ICT PSPs. However, no recommendations are made with respect to either limitation, as practical recommendations to limit connection of certified ICT PSPs to non-certified ICT PSPs require more ECCSs to be available, and the public availability of commercial copies of ICT PSPs, as well as ECCS security requirements and ICT PSP provider security usage documentation, may be considered necessary for the functioning of the EU internal market and the ECCS framework [1, recs. 1, 2, 4, 7, 40–42, 51, 80, 85, 93, 15, recs. 1–3].

3.4.2 Weaponisation

In the weaponisation phase, the attacker prepares the techniques, procedures and tools ('TPTs') for the attack, while the defender prepares their TPTs to defend against attacker TPTs [1, rec. 49, 85, p. 4].

Attacker weaponisation may be difficult for a certified ICT PSP to detect or deny, as it may occur without interaction with the certified ICT PSP [87, 89, 92, 93, pp. 199–200]. Where the attacker tests the weaponisation on a certified ICT PSP, detection and denial may occur via access limitation, data protection and usage logging, except when the attacker uses their own individual copy, for which they

[15] Depending on the security culture of the ICT PSP provider, the cost–benefit analysis may not support additional security.

have access rights, and which is isolated from the ICT PSP provider and target organisations [1, Arts. 51(a)-(c), (e)-(f)].

Defender weaponisation of certified ICT PSPs occurs during design and development through security by design and vulnerability identification [1, Arts. 2(14), 51(d), (g), (i), rec. 12]. This manifests in implementation of the minimum security objectives, without vulnerabilities, from early in design and development, both internal and external to the ICT PSP [1, Arts. 2(14), 51(a)-(j), rec. 12]. Defender weaponisation continues following the delivery of the certified ICT PSP, where security by default provides the initial configuration of internal and external security measures [1, Arts. 2(14), 51(i), rec. 13]. The interpretation of security by default as requiring that the security measures of a certified ICT PSP cannot be configured to a lower level of security than that required by the applicable ECCS is relevant here, as the initial weaponisation of the certified ICT PSP at an organisation may not meet the minimum security objectives without that interpretation. Protection of the security configuration by means of data protection, access limitation, usage logging and restorability allow persistence of the weaponisation state selected [1, Arts. 51(a)-(c), (e)-(f), (h), 43, p. 14].

Weaponisation continues in the maintenance of a certified ICT PSP, where secure updates provide fixes to identified vulnerabilities in the minimum security objectives [1, Arts. 2(14), 51(d), (g), (j)]. The recommendation that secure update patches not create new vulnerabilities in ICT PSPs is relevant here, as new vulnerabilities may compromise weaponisation. Weaponisation during maintenance also occurs through restorability, which restores availability and access to the implementations of the security objectives [1, Arts. 2(14), 51(h)]. The recommendation that restorability restore not only availability and access, but the full functionality of the implementations of the security objectives is important here, as without the full functionality, weaponisation may be compromised following restoration.

3.4.3 Delivery

Delivery is where the attacker moves tools for the attack to the target system [85, p. 4]. The defender seeks to detect and deny the delivery [85, p. 5].

Delivery to a target organisation or to a certified ICT PSP provider may take place via a certified ICT PSP, or to a certified ICT PSP—as its target destination. In each case, access limitation, data protection and usage logging, where it is monitored and acted upon, may detect and deny the delivery [1, Arts. 51(a)-(c), (e)-(f)]. Where an upstream ICT PSP is previously compromised in the delivery chain, such as through social engineering, and valid certified ICT PSP user access rights are obtained, access limitation and data protection would provide no detection or denial [44, pp. 2–3, 45, 117, pp. 145–146, 123]. This also applies where the certified ICT PSP is the target of social engineering for delivery [44, pp. 2–3, 45, 117, pp. 145–146, 123]. Usage logging may facilitate detection in both cases, where the usage logging data is monitored and acted upon, and attacker behaviour deviates from that expected of the valid user [44, p. 6, 45, 49, 51, 112, p. 2]. Where the target destination for delivery is a certified ICT PSP, restorability can restore a version of the ICT PSP that omits the delivery [1, Art. 51(h)]. Where the destination is a non-certified ICT

PSP connected to a certified ICT PSP, restorability of the certified ICT PSP will play no role, as the delivery will persist in the non-certified ICT PSP.

Social engineering and regular monitoring of usage logging data are limiting factors in the outcome efficacy of the minimum security objectives during the delivery phase, and, as will be seen, in subsequent phases. As they reflect how certified ICT PSPs are used, rather than inherent features, they may be considered external to the minimum security objectives, but within the control of organisations using certified ICT PSPs. It is therefore recommended that the legal benefits of organisations using certified ICT PSPs be tied, in implementing acts of the Cybersecurity Act, to regular monitoring of usage logging data and regular training to limit social engineering [1, Art. 49(7), recs. 8, 10, 93, 104, 117, p. 148, 123, pp. 34–37, 124, p. 401, 125, pp. 199–200]. The recommendations are also important to the outcome efficacy of the minimum security objectives, as they clarify the boundaries of certified ICT PSPs to users, promoting more secure use of certified ICT PSPs and supporting the trust and therefore the adoption of certified ICT PSPs [1, Arts. 1(1), 4(6), 54(1)(b), recs. 2, 7, 10, 65, 69, 78, 80, 93].

3.4.4 Exploitation

During exploitation an attacker exploits a vulnerability in the target system using tools transmitted during delivery, while the defender attempts to at least detect and deny the exploitation [85, pp. 4–5].

The ability of an attacker to exploit a vulnerability in an ICT PSP depends on the strength of reconnaissance and weaponisation, as well as the ability to deliver tools to the target system.[16] Where the minimum security objectives limit each of these, exploitation of a certified ICT PSP may be indirectly limited. The minimum security objectives can also directly limit exploitation, subject to the access rights the attacker obtains during delivery and exploitation.

Where the attacker obtains during delivery access rights that are valid for the certified ICT PSP being exploited, such as through social engineering, exploitation may only be detected and denied through monitoring and acting upon aberrations in usage logging data [37, paras. 26, 53, 38, paras. 22(3), 24, 31(3), 31(7), 44, pp. 2–3, 6, 45]. Where the access rights are not valid for a certified ICT PSP being exploited, access limitation, data protection and usage logging that is monitored and acted upon can provide detection and denial [1, Arts. 51(a)-(c), (e)-(f), 45]. Where a non-certified ICT PSP connected to a certified ICT PSP is the target of exploitation, the exploitation would occur without detection or denial by access limitation, data protection or usage logging of the connected certified ICT PSP. This is particularly important, again, as exploitation of the non-certified ICT PSP may enable the attacker to obtain valid access rights for the connected certified ICT PSP, including administrator level access rights [38, paras. 22(3), 24, 31(3), 44, 45, 49–52, 54, 109, paras. 15–16, 28]. An attacker may also obtain escalated valid

[16] Although it is common to focus on the exploitation phase, it is these precursor phases that are largely determinative of the outcome of the cyber attack.

access rights, including administrator level access rights, in the direct exploitation of a certified ICT PSP [44, pp. 2–5, 111].

Where the attacker is able to obtain administrator level access rights to a certified ICT PSP, the attacker may be able to control access limitation, data protection, usage logging, restorability and secure update data, services and functions, including modification of usage logging and restorability image data to limit detection of their previous and subsequent activities [38, paras. 22(3), 24, 31(3), 44, 45, 49–52, 54, 109, paras. 15–16, 28]. This augments the importance of the interpretation of security by default that certified ICT PSPs cannot be configured with a level of security below that required by the applicable ECCS. Where the exploitation of the certified ICT PSP occurs within services or functions of the minimum security objectives, those services or functions may no longer be operational, regardless of security objective configuration safeguards [38, paras. 22(3), 24, 31(3), 44, 45, 49–52, 54, 109, paras. 15–16, 28].

3.4.5 Installation

In installation, an attacker takes steps post-exploitation to maintain a persistent presence at the target system, while the defender is active in at least detection and denial [85, p. 5].

Installation occurs under the access rights obtained through exploitation [49, 52, 53, 55, 111–113, 115]. Installation may occur on a certified ICT PSP, where detection and denial operate to the extent access limitation and data protection limit those access rights, as well as the extent to which both remain functional after exploitation [1, Arts. 51(a)-(c), 45]. Usage logging may detect such activity and provide for detection and denial, subject to: how egregious the activity appears, the ability of the attacker to modify usage logging data and the extent to which usage logging remains functional following exploitation [1, Arts. 51(e)-(f), 43, p. 13, 44, p. 6, 49, 51, 110, p. 165, 112, p. 2, 113–115, 126, pp. 132–133, 127, p. 37]. Restorability will be able to restore a version of the ICT PSP that does not contain the installation, subject to the ability of the attacker to modify restorability image data and the extent to which restorability remains functional following exploitation [1, Art. 51(h), 49, 55]. Where installation remains undetected in the certified ICT PSP, restorability data images may contain the installation, providing for protracted presence of the installation following restoration. Where installation occurs in a non-certified ICT PSP connected to a certified ICT PSP, neither access limitation, data protection, usage logging nor restorability in the certified ICT PSP will provide for detection or denial of the installation.

3.4.6 Command and control

In command and control ('C&C'), the attacker obtains manual access to the target system, while the defender is active in at least detection and denial [85, p. 5].

The attacker may engage in C&C in person or by using automated mechanisms instructed by a central server or peer server [85, p. 5, 97, pp. 14–15, 17, 115, 128, pp. 14–20]. An exploited ICT product or service may also act as a peer C&C

server to coordinate C&C across a target organisation or across organisations in the EU internal market [49, 97, p. 18, 129, p. 183, 130–132]. The ability of the attacker to gain C&C is a function of the tools delivered, the extent of access rights obtained following exploitation and the extent of installation.[17] Where each is limited by the minimum security objectives, C&C can be limited; however, once C&C is obtained, the attacker can directly address the limitations, including through privilege escalation [43, p. 13, 49, 52, 111]. During C&C, the attacker is likely operating under valid access rights, unlimited by access limitation or data protection, and is only subject to detection and denial through monitoring of usage logging data, dependent on: how egregious the C&C activity appears, the ability of the attacker to modify usage logging data, the ability of the attacker to bypass usage logging services and functions, as well as the extent to which usage logging continues to function [1, Arts. 51(a)-(c), (e)-(f), 43, p. 13, 44, p. 6, 49, 51, 110, p. 165, 112, p. 2, 113–115, 126, pp. 132–133, 127, pp. 38–40].

3.4.7 Action on objectives

During action on objectives, the attacker takes steps to achieve the objectives of the attack at the target system, including compromising the availability, authenticity, confidentiality and integrity of ICT PSP data, services and functions [85, p. 5]. Action on objectives is where lateral movement across an organisation's network, or iterative penetration within an organisation's network, may occur [85, p. 5]. During this phase, the defender is focused on at least detection and denial [85, p. 5].

Detection and denial of action on objectives in a certified ICT PSP is based on the access rights the attacker is able to obtain with the certified ICT PSP and the extent to which the security objectives continue to operate [49, 52, 53, 55, 111–113, 115]. In light of the attacker having obtained C&C, detection of action on objectives and the previous phases is relegated to what the attacker allows to be detected. The capacity for lateral movement and iterative penetration is similarly based on the access rights the attacker is able to obtain and how these may assist with further delivery, exploitation, installation and C&C within the target organisation or across connected organisations in the EU internal market [44, pp. 2–6, 45, 46, 49–52, 54, 115].

From the legal perspective, while the phases leading up to action on objectives contribute to liability, action on objectives is where losses predominantly occur [85, p. 5]. Action on objectives is where personal data, trade secrets and other confidential data may be obtained from an organisation by an attacker, and where the operations of an organisation may be impacted, affecting compliance with service level agreements [85, p. 5, 97, pp. 10–11, 133, p. 71]. This further accentuates the importance of measures earlier in the kill chain from the legal perspective [78, pp. 6–7, 81, pp. 70–71, 85, p. 117].

[17] Each element contributes to the footprint of the attacker.

3.4.8 Damage assessment

During damage assessment, the attacker assesses the gains from the attack, while the defender assesses the losses from the attack.[18] Damage assessment forms the foundation for identifying the initial legal consequences of the attack and the initial legal options available.[19]

Damage assessment by the defender may only start once the defender has detected at least one phase in the attack, which may occur while the attack is still underway or some time after the attack ends.[20] Damage assessment by the defender may only be completed once the attack and associated vulnerabilities have been correctly understood.[21] Restorability data images, as a benchmark of the ICT PSP before the attack occurred, and usage logging data that may record attacker activity, both facilitate correctly understanding the attack and the associated vulnerabilities [41, 108, pp. 18, 26–27, 29, 31–32, 39, 41, 56, 67–69, 118, pp. 180–181, 134, p. 142]. The highly integrated nature of the minimum security objectives, where usage logging tracks access to and use of the data, services and functions of data protection, access limitation, restorability and usage logging, throughout the life cycle of the ICT PSP, assists with understanding how each security objective played a role in the attack, in order to appreciate the scope of potential damage [1, Arts. 51(e)-(f)]. The interpretation of the timeliness of restoration as being virtually immediate, and encompassing complete restoration throughout the life cycle of a certified ICT PSP, also augments damage assessment. The more frequent and complete the restorability data image snapshots, the more information is available to assist damage assessment across each stage of the life cycle of a certified ICT PSP.[22]

Damage assessment may not, however, be able to detect everything that occurred during an attack [43, pp. 11–15, 47, 49, 54, 55, 97, p. 13, 130, p. 11, 131]. Where the attack uses valid user access rights for a certified ICT PSP, such as through social engineering or through compromise of a connected non-certified ICT PSP, the ability to separate attacker activity from legitimate user activity may be challenging [126, pp. 88, 131–133, 127, pp 38, 40]. Where the attack uses the memory space of a certified ICT PSP, but not the APIs of the certified ICT PSP, which engage usage logging and restorability services and functions, attacker activity would not be recorded in usage logging or restorability image data.[23] The ability of the attacker to modify usage logging and restorability image data can also limit damage assessment [43, p. 13, 44, p. 6, 49, 51, 110, p. 165, 112, p. 2, 113–115, 126, pp. 38–40, 127,

[18] This is a fundamental and central phase from the practical perspective.

[19] Damage assessment is used to identify the losses, clarifying damages, as well as how the losses came to occur, clarifying liability, and who may have been involved, clarifying potential parties to legal proceedings.

[20] When damage assessment starts can play a significant role in defender tactics and the motivation to restore an ICT PSP.

[21] This understanding is necessary to understand where to look for potential and actual losses.

[22] The life cycle perspective is important as attacks and losses may occur across the stages of the life cycle of an ICT PSP.

[23] This may be detected by external security measures that operate during some stages of the life cycle of an ICT PSP.

pp. 180–181, 202, pp. 132–133]. The potential involvement of non-certified ICT PSPs in the attack further limits damage assessment from an organisation perspective, as usage logging and restorability image data may not be available for the non-certified ICT PSPs. Furthermore, organisation focus on other phases, such as a rush to engage in recovery to support organisation function and limit legal liability, can result in loss of data for damage assessment [108, pp. 38–39, 135, pp. 4, 6–7, 16, 136, pp. 129–130].

Damage assessment plays a significant role in subsequent phases. Recovery, communication and evidence gathering all depend on accurate damage assessment. The inability of damage assessment to identify all attacker activity limits recovery, as all of the effects to be recovered from may not be identified.[24] The inability of damage assessment to identify all attacker activity may also limit communication, as it may prevent identification of all relevant stakeholders to be notified, may prevent meeting reporting thresholds for notifying identified stakeholders and may result in incomplete communication content to identified stakeholders.[25] As communication can lead to legal proceedings by stakeholders against the organisation, this can limit the legal consequences to the organisation and the legal options of the stakeholders.[26] The inability of damage assessment to identify all attacker activity also limits the evidence available in the evidence gathering phase, further limiting legal consequences and options, as the evidence may not exist for specific procedural routes or substantive causes of action or defence.[27] Damage assessment can also impact evidence gathering by impacting the admissibility of evidence for legal proceedings.

Damage assessment and evidence gathering both focus on determining what occurred in an attack, but evidence gathering focuses on also being able to prove what occurred in an attack in legal proceedings.[28] The manner of damage assessment may impact the ability to prove what occurred in legal proceedings. The integrity and chain of custody of evidence may need to be proven in Court for evidence to be admissible, and damage assessment may inadvertently undermine the integrity and chain of custody of evidence [48, pp. 15, 18–19, 22–24, 30, 33, 40, 46–47, 108, pp. 15, 38, 40, 118, p. 148, 134, p. 96, 137, p. 224, 138, pp. 6–7]. This is particularly the case for transient evidence, such as evidence in the volatile memory of ICT PSPs [48, pp. 30–33, 135, pp. 4, 6–7, 16, 138, p. 4, 139, pp. 33–34, 147–149, 157, 140, pp. 3, 4–5]. The integrated nature of the security objectives supports being able to prove integrity and chain of custody through access limitation and data protection of both usage logging and restorability image data, as well as similarly protected usage logging of access limitation and data protection [1, Arts. 51(a)-(c), (e)-(f), (h)].

[24] It is likely common that not all attacker activity is identified.

[25] Limitations in communication to stakeholders in the broader internal market limit the ability of those stakeholders to recover and otherwise respond to attacks to limit the losses across the internal market.

[26] That lack of identification of attacker activity limits characterisation of losses to allow public policy to allocate the losses in line with social objectives as between the targeted organisation and the actual affected stakeholders.

[27] Particularly as against attackers and intermediaries, who are proximal in the chain of causation of losses.

[28] The distinction is practically important, as those performing the damage assessment may not be fully aware of the evidentiary requirements of the applicable procedural routes and substantive causes of action and defence.

3.4.9 Recovery

During recovery, the attacker and defender each seek to reduce the adverse consequences of the attack to themselves, including the legal consequences.[29]

The attacker seeks during recovery to reduce the evidence that could be used to identify them and their activity [43, p. 13, 44, p. 6, 47, 49, 55, 97, p. 6, 108, p. 29, 110, p. 165, 112, p. 2, 113–115, 131]. The extent of evidence to reduce depends on the extent of delivery, exploitation, installation, C&C and action on objectives [43, pp. 11–15, 47, 49, 97, p. 5, 130, p. 11]. Where a certified ICT PSP limits attacker reconnaissance, it can require the attacker to engage in more extensive delivery, exploitation, installation, C&C and action on objectives to compensate for the lack of reconnaissance, potentially creating more evidence for the attacker to reduce.[30] Where attacker reconnaissance is less limited, the attacker can be more efficient and streamlined in their TPTs, making recovery inherent in the TPTs and leaving little evidence to reduce following an attack. Usage logging and restorability image data are additional areas of evidence for an attacker to reduce; and where each are protected by access limitation and data protection, attacker evidence reduction may be more complicated and take more time [1, Arts. 51(a)-(c), (e)-(f), (h), 43, p. 13, 44, p. 6, 49, 108, p. 29, 110, p. 165, 112, p. 2, 113–115, 118, pp. 180–181]. The ability of an attacker to address usage logging and restorability image data depends on the attacker's ability to perform reconnaissance to understand each, as well as their ability to obtain access rights to either modify or bypass usage logging and restorability, such as through direct operating system calls rather than certified ICT PSP API calls.[31] The attacker activity of reducing evidence following an attack, or even during an attack, as opposed to having streamlined TPTs that automatically limit evidence, may in fact lead to attacker detection, accentuating the benefit of limiting attacker reconnaissance [108, p. 29].

From the defender perspective, similar to damage assessment, recovery may start once the attack is detected, and can only be completed once the attack and associated vulnerabilities are completely understood through damage assessment.[32] Where the attack leads to operational and legal consequences for an organisation, recovery would need to start and complete as soon as possible to minimise those consequences [136, pp. 129–130]. The ability of certified ICT PSPs to provide complete and virtually immediate restoration of access and availability, and the recommendation that they provide full functionality, in addition to access and availability, both facilitate rapid and complete recovery [45, 60, p. 12]. From an organisation perspective, however, the lack of such restorability in non-certified ICT PSPs that are identified

[29] Recovery may be seen as the primary goal of defenders, as legal routes may not be available.

[30] As the phases are sequential, leading to the attacker objective of action on objectives, there may be evidence in each phase, leading to an accumulated larger body of evidence to reduce.

[31] Ultimately it may not be possible for an attacker to reduce all traces, but rather limit the harm to them of the traces that remain.

[32] Particularly as evidence may be present in each phase of the attack, and the attacker may need to spend significant time locating and reducing the evidence from each phase with the added limitations of reduced reconnaissance in how to do that.

for recovery during damage assessment would delay restoration. Restoration may also be delayed by the fact that ICT PSP data processed during and following an attack, even in a certified ICT PSP, may not be reliable, and may need to be manually restored through repeated transaction processing against an older restoration image that damage assessment is able to verify is reliable.[33] Usage logging data in certified ICT PSPs can support such manual restoration, to the extent it is available and considered reliable following damage assessment. Finally, where data is copied or extracted from a certified ICT PSP during an attack, and is stored outside of an organisation, the restorability objective does not explicitly provide for retrieval of that data [60, p. 8, 102, pp. 11–15, 24–25, 103, p. 13, 104, pp. 210–213, 141, p. 93].

The need to recover as quickly as possible to limit operational and legal consequences may limit damage assessment, with the previously indicated consequential effects on communication and evidence gathering [108, pp. 38–39, 135, pp. 4, 6–7, 16, 136, p. 130]. The trade-off between recovery and each of the following: damage assessment, communication and evidence gathering, is minimized by the minimum security objectives. Complete restorability data images and usage logging data persist following restoration to indicate what was present before restoration, and what occurred during restoration. The evidence of what occurred during restoration further informs the damage assessment, communication and evidence gathering phases, and may be used to limit the legal consequences of the attack to an organisation [30, Art. 83(2)(c), 31, pp. 346–351, 33, pp. 172–173, 40, para. 44]. The loss of volatile data during restoration remains a consideration in the trade-off, as not all volatile data may also be present in usage logging or restorability image data [48, pp. 30–33, 112, pp. 3, 4–5, 135, pp. 4, 6–7, 16, 138, p. 4, 139, pp. 33–34, 147–149, 157].

The trade-off for non-certified ICT PSPs in the organisation appears to be less of a concern, as with the potential lack of usage logging or restorability image data, there may be less data to preserve to guide damage assessment in the first place. This, however, accentuates the need to preserve volatile data for non-certified ICT PSPs, accentuating the effects of the trade-off for non-certified ICT PSPs compared to certified ICT PSPs. As forensic copying of volatile data immediately following detection may not be a practical reality or priority for organisations across the EU internal market, the data available for damage assessment, communication and evidence gathering may be practically relegated to usage logging and restorability image data of certified ICT PSPs.[34] This practical reality allows restoration, damage assessment, communication and evidence gathering to be seen less as trade-offs for certified and non-certified ICT PSPs. This practical reality also allows for greater forensic readiness, which permits rapid damage assessment and evidence gathering to occur, without interrupting ICT PSP restoration or ongoing function [48, pp. 32–33, 136, pp. 118–119].

[33] The process of manual restoration may be error-prone, particularly where the manual process is not a common workflow in the organisation.

[34] It may be a challenge to expect this of SMEs for example.

3.4.10 Communication

Within communication, the attacker may communicate the attack to selected recipients, while the defender may report the attack to internal and external stakeholders, as well as authorities, on the basis of damage assessment and recovery.[35] Communication may also be used by the defender to guide the outcome of the attack by communicating directly or indirectly with the attacker in order to deceive or negotiate with them [37, para. 20, 55, 105, p. 36, 142, 143]. Communication starts to crystallise the legal consequences of an attack by notifying those who may seek legal proceedings against the organisation, or others, as a result of the attack.[36]

Communication by the defender may start at any phase once the attack is detected, but may only be completed with accuracy once damage assessment and recovery are completed.[37] Damage assessment and recovery inform communication, and limitations in each limit communication as previously indicated. This is important because the fact of communication, as well as the timing and content of communication may be used as evidence in legal proceedings to influence the liability of organisations [37, para. 66, 38, para. 31(6), 40, para. 44, 106, para. 34, 109, para. 59, 121, para. 46]. For example, communication by the defender may be legally required to occur within a specific timeframe, depending on thresholds informed by damage assessment and recovery, and include specific content determined through damage assessment and recovery [15, Arts. 14(3)-(7), 16(3)-(8), 16, Arts. 3–4, 30, Arts. 33, 34, 83(2)(h), 31, pp. 190–197, 346–351, 33, pp. 152–155, 164–167, 172–173, 34, Art. 13a(3), 35, Art. 19(2), 36, Arts. 40(2), 40(3), 144–146]. Where organisations are tempted to limit the content of the communication, usage logging data and restorability image data, protected by access limitation and data protection, and usage logging of each, are available to identify what organisations failed to disclose [1, Arts. 51(a)-(c), (e)-(f), (h)].

There is no requirement in the Cybersecurity Act for certified ICT PSP users to report certified ICT PSP vulnerabilities to either: certified ICT PSP providers, other users in the EU internal market that may be vulnerable or administrative bodies that monitor and enforce ECCS certification [1, Arts. 54(1)(m), 55(1)(c), 56(8), 63, 64, rec. 30]. It may be assumed that such reporting would occur at least by organisations to ICT PSP providers, as it would be in the best interest of the organisation

[35] Sharing of vulnerabilities and threats by attackers and defenders is very important as it is the basis for more extensive attacks across the EU internal market and improved defensive postures across the EU internal market.

[36] The stakeholder responses to communication can create further obligations on an organisation with respect to damage assessment and recovery, which may be to the detriment of other objectives during damage assessment and recovery.

[37] The balance of timing requires careful consideration of the potential practical and legal consequences of the communication, seeking to limit the overall losses to the organisation rather than losses across the EU internal market.

[38] This may not occur where it is a known, published vulnerability, which is of concern, as prioritization of the fix to the vulnerability can be proportional to the impact it has on ICT PSP users, and where ICT PSP users do not report that an incident has occurred with respect to the vulnerability, that can lead to a lower prioritization than it deserves.

with the vulnerability.[38] There is also no requirement in the Cybersecurity Act that certified ICT PSP providers have fixes for reported vulnerabilities available through secure updates within a specified timeframe following vulnerability identification [1, Arts. 51(d), (g), (j), 54(1)(m), 65, p. 26]. Where there is no requirement for a fix to be available in the EU internal market through secure updates within a specific timeframe, and where the vulnerability is known to attackers, including those who have already executed an attack using the vulnerability, organisations across the EU internal market are exposed to attacks using the same vulnerability for an unlimited period of time [78, p. 138, 120, pp. 13–16, 47, 55, 147, pp. 27–36]. The lack of a requirement that certified ICT PSP providers notify ICT PSP users, or other persons, including organisations, who may be adversely affected during this period undermines shared threat intelligence, which may otherwise operate to reduce the effects of the vulnerability across the EU internal market [1, rec. 7, 15, Art. 20(1), rec. 67, 16, Art. 2(d), rec. 40, 65, p. 26, 103, 148, p. 41, 152, pp. 97–103, 153, pp. 3, 5].

It is recommended that in implementing acts of the Cybersecurity Act, organisations be required to notify certified ICT PSP providers of vulnerabilities within a specific timeframe following first detection, and apply secure updates containing vulnerability fixes within a specific timeframe following their first availability, in order to retain the legal benefits of using certified ICT PSPs [1, Arts. 49(7), 54(1)(m), recs. 30, 104, 36, rec. 264, 46, 124, pp. 412–413, 154]. It is also recommended that the minimum security objectives of security by design, as well as vulnerability identification and documentation be augmented in ECCSs. First, certified ICT PSP providers should be required to design certified ICT PSPs in a modular fashion so that vulnerabilities in one part of the ICT PSP do not impact other parts of the ICT PSP, allowing a vulnerable part to be shut down until a fix is available, without impacting the rest of the function of the ICT PSP [61, pp. 99–107]. Second, certified ICT PSP providers should be required to commit to a specific turn-around time from vulnerability identification to fix availability through secure updates [1, Art. 54(1)(m)]. Third, certified ICT PSP providers should be required to notify certified ICT PSP users within a specific timeframe of configuration changes to isolate vulnerabilities until a fix is available via secure updates, without communicating further information that could facilitate wider attacker reconnaissance [1, recs. 30, 50, 155, pp. 24–27].

3.4.11 Evidence gathering

During evidence gathering the attacker may be passive, relying on their actions in previous phases to limit the evidence available against them.[39] The defender, however, is active and seeks to gather evidence of damage assessment, recovery and communication.[40]

[39] In spite of potentially being passive, limiting evidence is a primary objective for the attacker.

[40] This phase, as with the previous phases, may occur at different times for the attacker and for the defender, which is particularly important from the perspective of evidence gathering, where the attacker and defender are competing over the same evidence.

Defender evidence gathering may start as soon as damage assessment starts, continue through recovery and communication, and extend into legal proceedings. During legal proceedings, the defender may have to address requests for evidence by others engaged in legal proceedings against the attacker or the defender [15, Arts. 15, 17, rec. 61, 30, Art. 58(1), 31, pp. 285–289, 33, pp. 167–172, 34, Art. 13b, 36, Art. 41].

The ability to gather evidence for legal proceedings has been largely addressed in the analysis of damage assessment, recovery and communication. There is a further refinement that directly impacts legal proceedings: an imbalance in gathering identification evidence. Identification of parties is necessary to start legal proceedings against parties, or at least to obtain and enforce judgements against parties.[41] Usage logging data can assist organisations in identifying attackers, but is rarely sufficient on its own to identify attackers [102, pp. 15–16, 104, pp. 205–235, 129, p. 156, 157, 187, p. 107]. Usage logging services and functions are not explicitly permitted to track down and identify attackers in order to establish the 'whom' element of usage logging [1, Arts. 51(e)-(f), 60, p. 8, 102, pp. 11–15, 24–25, 103, p. 13, 104, pp. 210–213, 141, pp. 96, 98–100]. This creates an imbalance, because a defender organisation can rarely identify an attacker to start legal proceedings against that attacker, while the defender organisation may be required to communicate attacks to those affected by the attack, who may start legal proceedings against the defender organisation. As a consequence, defender organisations may be regularly exposed to losses through legal proceedings following cyber attacks, but rarely be able to offset their losses through legal proceedings against the attacker. This is important, because it changes the focus of evidence gathering for organisations from gathering evidence to pursue attackers to gathering evidence to defend legal proceedings.

In defending legal proceedings, organisations may be required to provide evidence that they prepared and implemented appropriate policies and procedures [15, Arts. 15(2), 17(2), recs. 60–61, 16, Arts. 4, 6, 30, Art. 58(1), 31, pp. 285–289, 33, pp. 167–172, 34, Art. 13b, 36, Art. 41, 57, pp. 14–15, 158, pp. 18–35, 159, pp. 10–26, 31, 160, pp. 14–28]. The minimum security objectives assist with documenting implementation as usage logging and restorability provide access limited and data protected tracking of ICT PSP configuration and operation. The interpretation of security by default as at least meeting the security requirements of an ECCS, and not allowing configuration of an ICT PSP below those requirements, also assists with establishing implementation, as the certified ICT PSP will always be configured to at least comply with the applicable ECCS. Usage logging and restorability image data also assist in determining where employees have deviated from documented policies and procedures, allowing an organisation to assert that the organisation should not be held liable for employees not following implemented policies and procedures [40, para. 44, 161, para. 51].

In defending legal proceedings, organisations may attempt to rely on cyber insurance to offset their losses.[42] To obtain cyber insurance, organisations may also

[41] In some jurisdictions proceedings may be started against unnamed parties to enable procedural routes for evidence gathering to assist further identification.

[42] Organisations may also attempt to rely on other existing insurance, but with less certainty.

be required to present documentation of planned and implemented policies and procedures [162, pp. 9, 14–15, 17–18, 163, pp. 25–27, 164, 165]. Usage logging and restorability image data, as well as security by default assist with establishing implementation to obtain cyber insurance [1, Arts. 51(e)-(f), (h)]. Organisations may not, however, always be able to rely on cyber insurance to limit losses from attacks, as the exclusion clauses may be broad and may be read broadly by insurers, leading to potential coverage disputes that can enter into their own legal proceedings [1, Arts. 51(e)-(f), (h), 62, pp. 145–148, 166, pp. 10–11, 167, pp. 90–94, 168, 169]. In coverage legal proceedings, usage logging and restorability image data may also be used by organisations as evidence to establish implementation of policies and procedures required for coverage.[43]

In defending legal proceedings, usage logging may provide organisations with evidence necessary to shift responsibility to intermediaries, or to pursue intermediaries independently to recover losses or limit future losses [170, 171].[44] While organisations may not be able to offset losses using this approach against intermediaries protected by liability legislation, organisations can obtain alternative relief, including through settlement with intermediaries, which supports organisation goals and deters future attacks [19, paras. 109–120, 20, paras. 119–124, 170, pp. 189, 194–195, 214, 171, p. 256, 172, Arts. 12–15]. Where the organisation can establish that the intermediary knew of the issue leading to the cyber attack and had the ability to prevent it, the intermediary may no longer be protected by liability legislation [19, paras. 109–120, 20, paras. 119–124, 172, Arts. 12–15]. The organisation can notify the intermediary to establish the knowledge element for future attacks, but may not be able to require the intermediary to monitor for such future attacks, undermining actual knowledge [172, Art. 15, 173, paras. 35–40, 47–53]. Furthermore, targeting intermediaries can negatively impact the reputation of an organisation [170, pp. 204–213, 171, pp. 250–260]. This augments the importance of gathering evidence, not to pursue attackers or intermediaries, but to defend against legal proceedings or pursue legal proceedings to assert insurance coverage.23, 16, Arts. 9–12, 30, Arts. 77, 79, 82–84, 31, pp. 335–338, 340–341, 344–354, 33, pp. 186–193, 167, pp. 66–90, 174, Arts. 1(1), 4(1), 5, 6–14, 16, 175, pp. 473–487, 176, pp. 489–493, 504–521].

3.4.12 Legal proceedings

Within legal proceedings the attacker avoids or defends the proceedings.[45] A defender organisation may be involved in legal proceedings in three ways: they may initiate legal proceedings, such as against an attacker, an insurer, an ICT PSP provider or an intermediary; they may cooperate in legal proceedings started by another entity,

[43] This will not assist, however, with the Court's reading of the breadth of policy coverage.

[44] This analysis does not include ECCS conformity of ICT PSP providers or ICT services, such as under Cybersecurity Act, Arts. 63–65, as ECCS conformity is treated as a control variable to facilitate outcome assessment.

[45] Avoidance of legal proceedings, while initially preferable, prevents the attacker from defending the case, which can result in Court orders to their detriment.

where they are not a party to the proceedings, such as criminal proceedings; and they may be a defendant in proceedings started by administrative bodies, or natural or legal persons [13, Arts. 15, 17–18,

In order to assess how the minimum security objectives contribute to legal proceedings, it is important to consider how the minimum security objectives contribute to the procedural routes and the substantive causes of action and defences in legal proceedings.[46] The ability of the minimum security objectives to contribute to procedural routes, causes of action and defences depends on the legal test that applies to each and the evidence required to meet each element of the legal test. The minimum security objectives may contribute to an element of a legal test by capturing specific evidence to support that element, or by their mere presence, through, for example, evidence of certification.

There is no requirement within the Cybersecurity Act that the minimum security objectives capture evidence to address the elements of any legal test for any procedural route, substantive cause of action or defence [1]. Even if an organisation attempts to use evidence created by implementations of the minimum security objectives to address an element of the legal test for a procedural route or substantive cause of action or defence, there is no requirement in the Cybersecurity Act that such evidence be considered admissible [1]. The minimum security objectives contribute to the integrity and chain of custody of evidence, which are relevant to the admissibility of evidence, as discussed previously, but do not explicitly satisfy any other admissibility requirements [1]. In other words, the Cybersecurity Act does not ensure that evidence gathered by the minimum security objectives can play a role in legal proceedings.

There is no requirement within the Cybersecurity Act that meeting the minimum security objectives satisfies or contributes to any element of any legal test for any procedural route, substantive cause of action or defence [1]. The fact of certification is permitted to act as a legal presumption, but that is not linked to any specific legal test for any procedural route, substantive cause of action or defence [1, Arts. 54(3)-(4)]. This may imply that the fact of certification is admissible in such legal proceedings, but the proceedings remain to be identified; and there is no explicit presumption of the admissibility of the fact of certification in other legal proceedings [1, 35, Arts. 3(33), 3(36), 25, 35, 41, 43, 46, rec. 22]. Furthermore, ECCS certification does not explicitly correlate with certification under other EU legislation that has legal weight [1, Arts. 54(3)-(4), rec. 74, 30, Arts. 32(3), 42]. Finally, the Cybersecurity Act encourages the use of international standards in the creation of ECCSs, but does not specify the legal effect of compliance with any international standard [1, Arts. 2(19), 8(1)(a), 62(4)(i), recs. 69, 76].

The Cybersecurity Act provides no explicit procedural safeguards for organisations in legal proceedings [1]. For example, there is nothing explicit in the Cybersecurity Act to prevent an organisation from having to defend legal proceedings in multiple EU Member States, or from being subject to duplicate remedies for the same cyber attack on a certified ICT PSP [1, Arts. 63–65]. Such procedural safe-

[46] The variations in each across EU Member States pose significant challenges to the harmonious effectiveness of the minimum security objectives in legal proceedings.

guards are available in a criminal context and are provided for generally for civil proceedings across the EU, as well as in specific administrative proceedings, but are not clearly established for administrative proceedings under the Cybersecurity Act [1, Arts. 63–65, 30, Art. 81, 177, Art. 4, 178, Arts. 29–34, recs. 21–24, 179, 180, para. 42].

The lack of explicit legal effect of meeting the minimum security objectives, as well as the lack of explicit provision for the admissibility of evidence obtained from and of the minimum security objectives, may reflect a legislative focus on securing ICT PSPs rather than on pursuing those who contribute to cyber attacks. This is particularly reasonable in light of the goal of protecting the EU internal market against cyber threats, as well as the limitations in identifying attackers and the interest in protecting innocent intermediaries [1, Arts. 1(1)(b), 46(1), recs. 1–3, 5, 102, pp. 15–16, 104, pp. 205–235, 156, 157, pp. 107–118, 172, Arts. 12–15]. The concern emerges that while there is no focus on targeting those who contribute to cyber attacks through legal proceedings, there is also no focus on protecting the organisations targeted by cyber attacks, during legal proceedings.

It is recommended that usage logging and restorability data be specified in ECCSs such that they comply with common evidentiary admissibility requirements for legal proceedings across the EU.[47] It is also recommended that a presumption of their admissibility, as well as the admissibility of ECCS certification to prove compliance with the minimum security objectives, be specified in implementing acts of the Cybersecurity Act. Finally, it is recommended that the legal effect of meeting the minimum security objectives through certification under an ECCS be explicitly identified in implementing acts of the Cybersecurity Act, such as in relation to the NIS Directive and GDPR [1, Arts. 54(2), 56(3), recs. 65, 74, 92]. The clarity is necessary not only for organisations defending legal proceedings, but also for decision makers in legal proceedings in order to consistently establish, in conjunction with the other recommendations on organisation practices and their legal effect in relation to certification, how certification balances with other organisation practices.

3.5 Conclusion

Qualitative model outcome analysis illustrates that the minimum security objectives provide organisations in the EU internal market using certified ICT PSPs with limited technical capability to resist and recover from cyber attacks, as well as with very limited legal capability to recover from cyber attacks.

The technical capacity is limited primarily by factors external to the minimum security objectives, but within the responsibility of targeted organisations, such as: training to limit social engineering, how often organisations monitor and act on usage logging data, delay in organisations notifying certified ICT PSP providers of vulnerabilities, delay in organisations applying ICT PSP vulnerability fixes, and connection of certified ICT PSPs to non-certified ICT PSPs in organisations. As these are factors within the control of organisations but outside the control of ICT PSP providers, it was recommended that the legal benefit of organisations using certified

[47] At least to address the case where organisations in the EU have to defend legal proceedings in the EU.

ICT PSPs be tied to organisation practices that limit the impact of these factors. In particular, it was recommended that implementing acts of the Cybersecurity Act require organisations to engage in the following practices to obtain legal benefit from using certified ICT PSPs:

1. Perform regular monitoring of certified ICT PSP usage logging data
2. Engage in regular training to limit social engineering
3. Report vulnerabilities to certified ICT PSP providers within a specified time after first detection
4. Apply certified ICT PSP fixes to vulnerabilities within a specified time after first availability

No recommendation was provided with respect to connection of non-certified ICT PSPs to certified ICT PSPs, as there are insufficient ECCSs currently available on which to practically base such a recommendation.

The technical capability of the minimum security objectives is limited secondarily by factors internal to the minimum security objectives, such as certified ICT PSP providers not being required to fix vulnerabilities within a specific timeframe or notify certified ICT PSP users of vulnerabilities within a specific timeframe. As these are factors internal to the minimum security objectives, they may be addressed by recommendations for ECCSs, in particular that certified ICT PSP providers be required to:

1. Design certified ICT PSPs in a modular fashion so that vulnerabilities in one part do not impact other parts of the ICT PSP, allowing a vulnerable part to be shut down until a fix is available, without impacting the rest of the function of the ICT PSP
2. Commit to a specific turn-around time from vulnerability identification to fix availability through secure updates
3. Notify certified ICT PSP users within a specific period of time of configuration changes to isolate vulnerabilities until a fix is available via secure updates, without communicating further information that could facilitate wider attacker reconnaissance

The technical capability is also limited by factors that are external to the minimum security objectives, but also external to the control of target organisations in the internal market, such as: public commercial availability of ICT PSPs, publication of ECCSs and publication of ICT PSP provider security usage details. Recommendations were not made with respect to any of these, as public commercial availability of ICT PSPs is important for the functioning of the internal market, and publication of ECCSs and ICT PSP security usage details are important for the functioning of the ECCS framework.

The ability of organisations to pursue and defend legal proceedings to limit losses from cyber attacks is limited by lack of clarity on the admissibility of evidence obtained from the minimum security objectives, as well as lack of clarity on the admissibility of evidence to establish conformity with the minimum security ob-

jectives, such as the fact of ECCS certification. In addition, there is no clarity on the legal effect of meeting the minimum security objectives, beyond permission to establish legal presumptions in EU and EU Member State law. It was recommended that:

1. Usage logging and restorability data be specified in ECCSs such that they comply with common evidentiary admissibility requirements for legal proceedings across the EU
2. A presumption of the admissibility of usage logging and restorability image data, as well as a presumption of the admissibility of ECCS certification to prove compliance with the minimum security objectives, be specified in implementing acts of the Cybersecurity Act
3. The legal effect of meeting the minimum security objectives through certification under an ECCS be explicitly identified in implementing acts of the Cybersecurity Act, such as in relation to the NIS Directive and GDPR

The potential impact of the limitations identified in qualitative model outcome analysis, as well as the potential impact of the recommendations to address them will be further illustrated through simulation analysis.

4 Cyber threat simulation analysis

4.1 Methodology

Cyber threat simulation will focus on cyber attacks, for the same reasons specified for model analysis. Cyber attack simulation will focus on the highest ranking threat vectors and highest ranking threat actors for organisations in the internal market, as identified in ENISA threat landscape reports from 2012 to 2018 [76–78, 148–151]. ENISA threat landscape reports are selected for threat prioritisation, as ENISA was responsible from at least 2013 onwards for supporting EU network and information security policy and law [181, Arts. 1(3), 2(2), 3(1)(a), recs. 2, 3, 12, 13, 19, 24]. The attacks will be described with reference to the phases of the modified LM-CKC to provide correlation with model analysis. The attacks to be simulated include: a ransomware attack, an insider attack, a cyber espionage attack, a denial of service and data breach attack and a nation state monitoring attack.

Where the simulations rely on newly discovered vulnerabilities, it is important for outcome efficacy analysis to note that locating new vulnerabilities in ICT products and services is not difficult, as there may be vulnerabilities in ICT products and services at any one point in time that can be located by evaluating ICT products and services against common weakness enumerations [48, pp. 8–10, 55, 111, 120, pp. 15–17, 182, 183].

4.2 Ransomware attack

Ransomware is a type of malicious software ('malware') that denies access to ICT PSP data, services or functions until a ransom is paid [143]. Malware was the highest ranking threat from 2014 to 2018, and ransomware was the most prevalent type of malware in 2018 [76, p. 7, 77, p. 9, 78, pp. 9, 24, 31, 150, p. iv, 151, p. 7]. The majority of malware attacks occur through email, including phishing, where a person is lured to a website that contains the malware [78, pp. 31, 40, 67, 72, 102, 119]. Web-based attacks were the second ranking threat from 2014 to 2018 [76, p. 7, 77, p. 9, 78, p. 9, 150, p. iv, 151, p. 7]. Cybercriminals were the most engaged cyber attacker from 2016 to 2018 and were responsible for over 80% of the cyber attacks detected in 2018 [76, p. 69, 77, pp. 93–94, 78, pp. 119].

In this simulation, a cyber criminal targets organisations in the EU internal market with spam emails linked to a website containing ransomware [78, p. 105]. The ransomware is designed to target vulnerabilities in an operating system used by organisations in the EU internal market. The operating system is certified under an ECCS and, as such, meets the minimum security objectives.

The cyber criminal performs reconnaissance by reviewing published historical vulnerability reports of a commonly used version of the operating system in the EU internal market, as well as the source code of the same version made available to the open source community by the operating system provider. The cyber criminal identifies a new vulnerability that is not present in the historical vulnerability reports. Neither the operating system provider nor the organisations to be attacked detect the attacker's reconnaissance. An organisation using the targeted version of the operating system performs reconnaissance by reviewing the same historical vulnerability reports. The organisation does not review the source code for vulnerabilities or perform vulnerability or penetration testing [184]. The operating system provider tests the operating system to ensure it meets the requirements of the ECCS, including that published vulnerabilities are fixed, but does not review the source code to identify further vulnerabilities.

During weaponisation, the cyber criminal uses existing ransomware code that is available in attacker communities and modifies it to target one historical vulnerability and the newly discovered vulnerability in the target version of the operating system [52, 78, p. 101]. The cyber criminal tests the ransomware against a commercially available copy of the operating system obtained under a pseudonym. The cyber criminal registers a URL that appears similar to, but is different from a legitimate organisation's URL, using another pseudonym. The cyber criminal prepares a web page that is similar to the webpage of the same legitimate organisation, but is scripted to download and automatically execute the ransomware. The cyber criminal places the web page and the ransomware on a server whose IP address is registered with the URL and which resides in a jurisdiction with limited legal options for organisations in the EU internal market. The cyber criminal constructs a spam email that is likely to entice people to click the website link in the email and places the email within an existing spam bot network for distribution [78, pp. 43, 54–56, 58]. Weaponisation by the operating system provider occurs through compliance with the applicable ECCS, including provision of fixes to known vulnerabilities in the target version

[1, Art. 51(g)]. Weaponisation by the organisation occurs by applying those fixes through the secure update process [1, Art. 51(j)].

Delivery starts when the spam bot transmits the email to an employee in the organisation. The employee receives the email and clicks the link in the email. The employee's web browser opens the illegitimate web page, which automatically downloads and executes the ransomware on the employee's computer using the employee's access rights. The operating system records the storage and execution of the ransomware [1, Arts. 51(e)-(f)]. The ransomware attempts to exploit the known vulnerability and is not successful as the organisation has applied the fix to the known vulnerability. The exploitation of the newly discovered vulnerability is successful and allows the ransomware to escalate privileges to root level administrator rights, with full access rights across the organisation [53, 113]. The operating system records the attempted exploitation of the known vulnerability and the successful exploitation of the new vulnerability [1, Arts. 51(e)-(f)]. The ransomware uses the valid administrator rights obtained to install itself across the organisation via peer-to-peer C&C [55, 113]. The operating systems across the organisation record this activity, but during C&C the ransomware automatically deletes all operating system usage logging and restorability image data across the organisation, including that of the initiating employee [55, 113]. The ransomware engages in action on objectives by encrypting data across the organisation and presenting a ransom note [53, 55, 113, 114, 154, 184].

Access limitation and data protection provide no limitation from delivery to action on objectives, as the attacker activity occurs under valid access rights [1, Arts. 51(a)-(c)]. Usage logging records the activities from delivery to action on objectives, but usage logging data is automatically deleted by automated C&C [1, Arts. 51(e)-(f), 54, 113, 154]. The rapid, automated operation of the ransomware results in the usage logging data not being assessed between delivery and action on objectives. If the usage logging data were assessed, delivery may appear within the normal behaviour of the employee—clicking on links in emails and downloading files from web pages with apparently legitimate URLs [126, pp. 88, 131–133, 127, p. 38–40]. Exploitation would appear aberrant as it results in root access followed by file system activity under root access, but may be indistinguishable from a system error initially, and may be obfuscated by large amounts of operating system usage logging data [1, Arts. 51(e)-(f), 48, p. 36]. Investigation of the distinction would need to start and complete rapidly to lead to detection before automated peer-to-peer C&C deletes usage logging data.

In damage assessment, the attacker checks for payment, while the organisation evaluates the spread of the ransomware by comparing the extent of encrypted data to the most recent offline restorability data image [55, 113, 114, 118, pp. 180–181, 184, 185, para. 15]. Assessment of attacker activity is limited by the deletion of usage logging and restorability image data, as well as by the timeframe between the most recent offline restorability image data and the delivery of the ransomware. The organisation engages in recovery by applying the most recent offline restorability data images in an isolated network, but is unable to manually bring the network completely up to date in light of deletion of usage logging data on the exposed network [54, 53, 113, 114, 118, pp. 180–181, 154, 184, 185, para. 15].

The organisation engages in communication by notifying the relevant data protection authority and the operating system provider on the basis of damage assessment, but delays in notifying data subjects [30, Arts. 33, 34, recs. 85–88, 31, pp. 192–193, 33, pp. 164–166]. In light of limited damage assessment, it takes more time for the operating system provider to identify and fix the vulnerability.[48] The cyber criminal in the meantime can continue the attack on other organisations in the EU internal market. When the fix is made available, it protects against exploitation of the new vulnerability, but does not remove the ransomware or decrypt organisation data.

During evidence gathering, the relevant data protection authority may request full access to all usage logging and restorability data for their own forensic report to be prepared [38, para. 19]. Only offline restorability data images, which include usage logging data, would be available to assist with this. The organisation attempts to gather evidence to identify the attacker, limited by encryption of organisation data and attacker use of pseudonyms [186–188].

In legal proceedings, the data protection authority pursues administrative action, which the organisation attempts to defend by showing diligent application of patches to the target version of the operating system as evidenced by historical, offline usage logging data of secure updates [1, Arts. 51(e)-(f), (j)]. In light of the lack of clarity on the admissibility of that evidence and its legal effect, further analysis lacks sufficient foundation, reflecting legal uncertainty in the defence of the organisation.

In this simulation, social engineering enables delivery, but the capacity for extensive, undetected and unlimited reconnaissance of the certified ICT PSP is determinative. Reconnaissance allows the attacker to find a new vulnerability, to automate its exploitation, to automate installation and peer-to-peer C&C, including usage logging and restorability image data deletion, and to automate action on objectives, allowing a rapid attack that limits detection and denial. Furthermore, limitation of damage assessment through encryption and deletion of usage logging and restorability image data delays vulnerability identification and fixing, allowing attacks to continue across the EU internal market. The simulation exemplifies the importance of social engineering training to prevent attacks, as well as least privilege access right configuration and network segregation to limit the spread of attacks [113, 154, 184]. It is recommended that the legal benefits of organisations using certified ICT PSPs be tied to organisations implementing least privilege access right configurations in certified ICT PSPs and network segregation of certified ICT PSPs [1, rec. 104].

4.3 Insider attack

Insiders were the second most engaged cyber attacker from 2016 to 2018 [76, p. 69, 77, p. 94, 78, pp. 69–70, 120]. The majority of insider attacks from 2014 to 2018 involved misuse of access rights and access of internal networks, and in 2018 preferentially targeted confidential corporate information, access credentials, sensitive personal information and intellectual property on corporate databases and file servers [78, pp. 71, 120, 108, pp. 45–46].

[48] It may not be possible to locate the vulnerability.

In this simulation, the insider is an employee of a corporation. The insider targets confidential corporate business information, access credentials, customer and employee personal data, as well as trade secrets on corporate databases and file servers. The databases and the operating systems of the file servers are certified under ECCSs, and as such meet the minimum security objectives.

The insider performs reconnaissance through their own job-related use of corporation databases and file servers, as well as by monitoring other employees and contractors to observe their access rights, access credentials and behaviour patterns. The employee observes where paper copies of access credentials (as memory cues), confidential business information, personal data and trade secrets from the certified database and file servers are stored or discarded. The employee develops a reputation for being on their cell phone at work and uses the reputation to record other employees and contractors, including system administrators repairing workstations as they enter their file server workstation and internal database credentials [108, pp. 55–56]. The minimum security objectives of the databases and file servers do not detect or deny such reconnaissance.

The insider weaponises by preparing a username and password list of target employees and contractors, encrypting the list, placing the encrypted list on their cell phone and bringing the cell phone and a flash drive into work [108, pp. 11, 28–31, 44, 56]. The organisation databases and file server operating systems are weaponised with implementations of the minimum security objectives. Delivery occurs when the insider accesses the work premises with their cell phone and flash drive on a day when the target employees or contractors are normally present, but when the insider knows that they will not be present—such as on sick days. The phases from exploitation to action on objectives occur rapidly. The insider takes cell phone photos of target employee access credential memory cues and other documents on their desk and obtains copies of documents in their recycling bin and common recycling bins. The insider then selects an unused, isolated workstation to download data from internal databases and file servers to their flash drive using target employee credentials. Action on objectives is complete when the employee leaves the premises of the corporation with their cell phone, flash drive and obtained paper documents.

Access limitation and data protection of the target databases and file servers would not detect or deny the insider at any phase from delivery to action on objectives as the insider is using valid access rights [1, Arts. 51(a)-(c)]. Usage logging may detect access to large amounts of data in a short period of time from unfamiliar workstations, but that would need to be monitored frequently by the corporation to allow for detection and subsequent denial by the corporation [1, Arts. 51(e)-(f), 40, paras. 36(3), 41(2), 41(6), 108, pp. 18, 26–27, 29, 31–32, 39, 41, 56, 67–68, 189, pp. 20–23]. Insider photographing and acquisition of printed memory cues and printed data from the internal databases and the file server operating systems would not be detected or denied by access limitation, data protection or usage logging as they occur offline.

Damage assessment by the insider occurs when the insider assesses the cell phone images, paper documents and flash drive contents. Damage assessment by the corporation may start once the corporation is aware of the attack. As credentials were

taken in the attack, the attack may be repeated several times until detected, including by different threat actors, such as cyber criminals that obtain the credentials from the insider [40, para. 22, 189, p. 29, 190]. Usage logging of the internal databases and file servers assists damage assessment, limited by the ability to distinguish insider activity from authentic user activity and the fact that substantial amounts of data may have been obtained via cell phone photographs, cell phone recordings and discarded paper documents [1, Arts. 51(e)-(f), 126, pp. 88, 131–133, 127, pp. 38, 40]. Where the target employee and contractor credentials are the same on non-certified ICT PSPs in the corporation, usage logging data may not assist with damage assessment of those ICT PSPs.

In the recovery phase, the corporation may change the access credentials of all employees and contractors, tighten access rights on a least privilege basis and implement stronger physical security measures [45, 78, pp. 72–73, 97, pp. 15, 17–18, 108, pp. 28–31, 44, 56, 161, paras. 22, 33, 38, 57]. Restorability of the internal databases and file server operating systems would not be of assistance as data was copied, not modified or deleted, and would restore the credentials copied by the insider. The corporation may attempt to locate, obtain and delete external copies of the data obtained and distributed by the insider, but the restorability objective does not explicitly extend to facilitating such activities [1, Art. 51(h), 60, p. 8, 102, pp. 11–15, 24–25, 103, pp. 13, 104, pp. 210–213, 141, pp. 98–100].

In the communication phase, the corporation reports the events in line with legal obligations, subject to the limitations of damage assessment with respect to separating legitimate user activity from insider activity and the inability to assess cell phone recordings, cell phone photographs and paper documents taken by the insider. Evidence gathering would similarly be limited by damage assessment, and in particular, as valid credentials were used, neither access limitation, data protection nor usage logging would directly identify the insider [1, Arts. 51(a)-(c), (e)-(f)]. In the absence of insider identification, the corporation can only defend legal proceedings. In legal proceedings, the corporation may lead evidence of the fact of certification of the targeted database and file system operating system, as well as usage logging data to indicate that each had appropriate configuration settings, at least complying with certification [1, Arts. 51(e)-(f)]. In light of the lack of clarity on the admissibility of that evidence and its legal effect, further analysis lacks sufficient foundation, reflecting legal uncertainty in the defence of the organisation.

In this simulation, reconnaissance plays a significant role again, as does organisation monitoring of usage logging data, but the distinguishing feature is how access limitation, data protection and usage logging address physical security. Access limitation may limit who can view access credentials in a certified ICT PSP and who can print data from a certified ICT PSP, for example, but cannot limit people from writing down their access credentials on paper, and cannot directly limit the handling of printed data. Usage logging can detect aspects of the insider attack, but is dependent on the ability to discern abnormal user behaviour from normal user behaviour, and is unable to record the taking of photographs or access to and use of paper documents [108, pp. 18, 26–27, 29, 31–32, 39, 41, 56, 67–68, 189, pp. 20–23]. Standard physical security measures, such as limiting access within offices, limiting paper documents to locked cabinets and locked recycling bins, as well as limiting

flash drive usage at workstations may have assisted the organisation in this simulation [45, 97, pp. 15, 17–18, 108, pp. 28–31, 44, 56, 161, paras. 22, 33, 38, 57]. It is recommended that implementation of physical security measures surrounding the use of certified ICT PSPs be linked to the legal benefit that organisations may obtain through use of certified ICT PSPs [1, rec. 104].

4.4 Cyber espionage attack

Cyber espionage is performed by some of the most capable threat actors, including APT actors, at the request of corporations or nation states [54, 78, pp. 107–109, 129, pp. 187–188, 192, 196–197, 131, 132]. Cyber espionage is also performed by cyber criminals and by insiders seeking to establish competing enterprises [78, pp. 107–109, 108, p. 24]. Each of these threat actors were among the most engaged threat actors from 2015 to 2018 [76, pp. 70–71, 77, pp. 94–95, 78, pp. 107, 120–121, 151, pp. 55–57].

Cyber espionage in 2018 tended to use spear-phishing emails to motivate recipients to open attachments containing malware or to click on links to websites containing malware [78, pp. 40–42, 113]. Phishing, including spear-phishing, was the fourth ranking threat in 2017 and 2018 [77, p. 9, 78, pp. 9, 24, 31, 67, 72]. Cyber espionage uses a variety of malware, including spyware and remote access trojans ('RAT's) [54, 129, pp. 187–207, 131, 132]. Spyware tracks user action and accesses data on ICT products and services [191]. Spyware was the third most used malware between 2017 and 2018 [78, pp. 27, 31, 33]. RATs open back doors into ICT products and services to allow surveillance of users [192]. RATs were the fourth most used malware between 2017 and 2018 [78, pp. 27, 31, 33]. Spyware and RATs may be combined into hybrid malware with both capabilities for cyber espionage [46, 47, 49–51, 115, 129, pp. 191–197, 199–201, 204]. Malware used for cyber espionage often avoids detection by running in a 'fileless' manner—in the process space of an ICT product or service and by rewriting its own code [78, pp. 26–29, 118, 129–130].

In this simulation, a cyber spy engages in spear-phishing to get an employee with access to trade secrets in an organisation to open an email attachment that downloads and executes RAT spyware [78, pp. 40–42, 113]. The attachment used by the cyber spy is typically opened by a word processing application common in the EU internal market. The RAT spyware uses a vulnerability in the word processor to locate and retrieve trade secrets on the organisation's file system. The word processor is certified under an ECCS and, as such, meets the minimum security objectives.

The cyber spy performs reconnaissance on the organisation to identify which employees may have access to trade secrets [49, 93, p. 199, 97, p. 14, 129, pp. 206–207]. The individuals are selected and further reconnaissance is performed on them to assess their interests, behaviour and cyber hygiene [49, 93, p. 199, 97, p. 14, 129, pp. 206–207]. The reconnaissance is not detected by the target organisation [87, 97, p. 3]. The cyber spy acquires a copy of the word processor pseudonymously and identifies a new vulnerability. This is not detected by the target organisation or the word processor provider. During defender reconnaissance, the word processor

provider is aware of macro execution as an attack vector, and the target organisation tracks updates from the word processor provider diligently.

The cyber spy weaponises by modifying custom RAT spyware to exploit the vulnerability. The cyber spy then creates a legitimate looking word processor document with a macro that downloads and executes the RAT spyware in-process with the word processor [97, p. 4, 129, pp. 204–205]. The cyber spy carefully creates an email that will encourage the recipient to open the email and the attachment. The email and word processor document are both prepared using careful language and metadata control to limit detection [129, pp. 185, 189, 198–199]. The cyber spy prepares previously compromised civilian computers with bots to act as intermediaries in the attack and places the crafted email, word document and RAT spyware on these proxies [87, 115, 129, pp. 186, 198–200, 205–206]. The word processor is weaponised, by default, to warn users before macros execute, access the internet and download files.

The cyber spy delivers the email with the attachment to the target employee via one of the proxies, on a specific day of the week and at a specific time of the day to optimise social engineering [78, p. 43]. The employee opens the email and the attachment, disregarding the familiar word processor warnings about macro execution.[49] The macro executes, downloading and executing the RAT spyware, which exploits the vulnerability in the word processor to install itself in the process space of the main word processor thread rather than the macro thread. The RAT spyware opens an encrypted C&C channel on the port, protocol and encryption standard used by the word processor for secure updates, but using the cyber spy's encryption key [78, p. 26, 97, p. 5, 115]. The RAT spyware does not engage in further installation in order to minimise its presence on the target system and limit detection [49, 129, pp. 189, 204–206]. The RAT spyware does, however, automatically delete word processor log file entries regarding macro execution, internet access and download, and does corrupt, but does not delete, the applicable restorability image data of the word processor that would contain the same log file entries [49, 51, 115, 129, p. 207].

During action on objectives, the RAT spyware automatically locates, retrieves and encrypts copies of potential trade secrets via the C&C channel through the proxies. The cyber spy assesses the gains of the attack and engages in further brief manual location and retrieval of trade secrets via the C&C channel and proxies. The RAT spyware then rewrites the code in the macro to make it unremarkable, and obfuscates then carefully deallocates memory in the process spaces used to limit physical memory forensic analysis [48, pp. 30–32, 35]. The cyber spy removes traces of the activity on the civilian proxies [129, pp. 191, 199, 207].

Access limitation and data protection of the word processor are not able to detect or deny cyber spy activity in either phase, as the activity operates under the valid access rights of the target employee [1, Arts. 51(a)-(c), 49, 126, p. 132]. Usage logging data of macro execution, internet access and download were removed automatically following macro execution, limiting detection through monitoring usage logging data [1, Arts. 51(e)-(f)]. Restorability data images with unmodified usage logging data were corrupted, preventing detection through their review [1, Art. 51(h)]. Usage

[49] Even with good cyber hygiene, there can be user fatigue with repetitive security measures.

logging of the word processor would not detect any further activity of the RAT spyware, as the RAT spyware uses the process space of the word processor to execute, including port activity for C&C, through direct operating system calls—without using the word processor APIs that engage usage logging or restorability.[50]

Damage assessment at the target organisation can only occur once the attack has been detected, and that may not occur for some time, or at all, given the deletion of usage logging data [127, p. 39]. Damage assessment, once started, would not identify any information about the attack, as usage logging data contains no record of the activity, restorability image data is corrupted, the macro code was rewritten, volatile memory was obfuscated and deallocated, and all traffic was encrypted using an encryption key not available to the organisation. The subsequent phases of the modified LM-CKC would therefore not be engaged by the defender organisation, as there is no indication of what to recover, communicate or gather evidence in relation to, and as such no legal proceedings to engage.

In this simulation, the strength of attacker reconnaissance on their private copy of the certified ICT PSP allows the attacker to automate log file and restorability data image compromise to limit detection, as in the ransomware attack, but also to use the secure update mechanism of the certified ICT PSP as part of its weaponisation for C&C and action on objectives. A weakness in security by default is also illustrated, as an employee frequently presented with warnings through security by default may eventually disregard the warnings by default [193]. Regular training of employees on social engineering can potentially assist with this [55, 125, pp. 199–200, 184]. In this simulation it is the absence of evidence, rather than the lack of clarity about the admissibility of evidence or the legal effect of admissible evidence, that limits the organisation's ability to address the losses from the attack through legal proceedings.

4.5 Denial of service and data breach attack

Hacktavists were the fourth most engaged cyber attackers from 2016 to 2018 [76, pp. 69–70, 77, p. 95, 78, p. 121]. Hacktavists focus on bringing attention to specific issues by obtaining and exposing confidential organisation information, defacing organisation websites and executing denial of service attacks on organisation servers [78, p. 121]. In 2018, hacktavists tended to use web application attacks using SQL injection (querying internal databases through websites), and were the main threat actors engaging in denial of service attacks [78, p. 121, 194]. Web application attacks were the third ranking threat from 2014 to 2018, and SQL injection was the most common type of web application attack in 2018 [76, p. 7, 77, p. 9, 78, pp. 9, 37–39, 64, 67, 150, p. iv, 151, p. 7]. Denial of service attacks were among the top six cyber threats from 2014 to 2018, and in 2018 preferred to target the UDP, TCP and NTP protocols [76, p. 7, 77, p. 9, 78, pp. 9, 47–49, 51–52, 150, p. iv, 151, p. 7].

In this simulation, a hacktavist uses SQL injection to gather confidential corporate data from a publicly accessible corporate website connected to an internal corpo-

[50] The operating systems in this simulation are not certified, and if they were, they may not detect file system access of documents a user has access rights to from a word processing program as being an anomaly.

rate database, then executes a distributed denial of service attack against corporate servers via the corporate external firewall, using the UDP, TCP and NTP protocols simultaneously. The internal database and firewall are certified under separate ECCSs, and as such each meets the minimum security objectives.

During reconnaissance, the hacktavist locates a publicly available corporate website contact form that allows entry of data into the corporation's contact management database. The hacktavist then locates a distributed denial of service package in an attacker community market, which uses a botnet to target the UDP, TCP and NTP protocols [48, p. 8, 78, pp. 47–49]. Finally, the attacker locates a public location with free Wifi access from which to initiate the attacks. The target corporation and providers of the database and firewall do not detect the hacktavist's reconnaissance. The firewall provider is aware of distributed denial of service attacks against firewalls using the UDP, TCP and NTP protocols.

The hacktavist weaponises by preparing SQL queries and by acquiring access to the distributed denial of service package via the attacker community market [48, p. 8, 78, pp. 47–49]. Again, neither is detected by the corporation, the database provider or the firewall provider. The firewall provider, through security by design, has incorporated measures into the firewall to ensure the availability of stored and transmitted data during distributed denial of service attacks using the UDP, TCP and NTP protocols [1, Arts. 51(a)-(b), (i)].

The phases from delivery to action on objectives occur rapidly for the SQL injection attack, from delivery of the queries to the corporate website and exploitation of the internal database under the access rights of the web application to action on objectives where the hacktavist retrieves detailed contact management information on clients of the target corporation. Database access limitation and data protection are not able to detect or deny the queries as they are performed using valid access rights provided by the web server [1, Arts. 51(a)-(c)]. The queries may not be valid initially, depending on the sophistication of the hacktavist, which increases the chance of detection in usage logging data prior to valid queries being entered [1, Arts. 51(e)-(f)]. Queries that illustrate a lack of awareness of the database schema are not expected from a programmed web application for data input.[51] Detection and denial of the SQL injection attack depends on how often the corporation monitors usage logging data to detect abnormal invalid queries and abnormal valid queries [46, 48, p. 21, 50].

The attacker then proceeds to the distributed denial of service attack to distract the corporation from the SQL injection attack. The phases from delivery to exploitation in the denial of service attack occur rapidly: the hacktavist executes the attack from the botnet, but as the firewall is designed and developed through security by design and configured through security by default to detect and deny such attacks, the distributed denial of service attack is automatically detected and denied in the delivery and exploitation phases.

Damage assessment by the hacktavist involves reviewing the database query results. Damage assessment by the target corporation starts once the data breach or

[51] Changes in the code or schema that result in lack of alignment can occur outside of an attack, but lack of alignment is not likely when neither the code nor the schema has been changed.

denial of service attacks are detected. Usage logging data by both the database and firewall assist significantly with each, as they track attack activity in detail and, for the database specifically, can be compared to the programmed queries of the web application [1, Arts. 51(e)-(f)]. The corporation may engage in recovery by taking the contact form web page down from the website, disabling requests under cached versions of the web page until the SQL injection vulnerabilities are fixed and engaging in firewall scrubbing [195, pp. 6–7, 9]. Again, there is no explicit provision in the restorability objective for organisations to retrieve data copied and taken outside of the organisation [60, p. 8, 102, pp. 11–15, 24–25, 103, p. 13, 104, pp. 210–213, 141, pp. 96, 98–100].

In the communication phase, the corporation reports the data breach in accordance with its legal requirements on the basis of detailed damage assessment, including to a data protection authority [109, para. 59]. The hacktavist may communicate the data breach within their community, including the contents of the data obtained. The denial of service attack is not communicated by the organisation or the hacktavist as it was not successful.

During evidence gathering, usage logging data of the firewall would identify the botnet IP addresses as the source of the denial of service attack, but no more. Usage logging of the database would record the data retrieved by the hacktavist, but as the web server connected to the internal database was not certified in this simulation, there may be no record of the hacktavist IP address to link to firewall usage logging data. In the absence of such identification evidence, the corporation would not be able to start legal proceedings against the hacktavist, but may consider legal proceedings against the intermediary hosting service of the botnet IP addresses [170, 171]. The corporation, depending on the data obtained by the hacktavist, may be subject to legal proceedings by a data protection authority. In defending such legal proceedings, the corporation may lead evidence of ECCS certification of the database to assert that they took appropriate technical and organisational measures [30, Art. 32, 31, pp. 187–188, 33, pp. 114–115]. The legal effect of database ECCS certification weighed against the SQL insertion vulnerability in the connected web server is not clearly established with respect to liability, or as a mitigating factor in assessing penalties, to provide a sufficient foundation for further analysis [109, paras. 15, 28(a), 43, 45, 48, 50].

In this simulation, weaker attacker reconnaissance of target ICT PSPs leads to attacks that are more easily detected and denied and that support damage assessment and communication more extensively. The frequency of organisation monitoring of usage logging data plays a significant role again in detection and denial, specifically with respect to the database attack. Again, the absence of clarity on the admissibility and the legal effect of certification leads to uncertainty in how the fact of certification may be balanced against other factors, such as exploitation of a connected non-certified ICT PSP, in assessing liability and damages.

4.6 Nation state monitoring attack

Nation states may monitor and control ICT PSPs to protect national interests [196, p. 13]. This type of attack is particular in that nation states rely on vulnerabilities

in ICT PSPs, rather than discourage vulnerabilities in ICT PSPs [46, 50, 154]. Furthermore, the ICT PSP provider, instead of being aligned with their ICT PSP user, may be aligned with the nation state targeting their ICT PSP user [61, pp. 5–7, 11–19]. A nation state may, for example, request that an ICT PSP provider give it the means to bypass security measures, such as an encryption key, or may request an ICT PSP provider to create specific vulnerabilities that only the nation state and ICT PSP provider are initially aware of [196, pp. 12–15, 19–20, 22, 25–27, 197–201]. This differs from cyber espionage based on the potential for collusion. In cyber espionage, the ICT provider and nation state are opposed, while in nation state monitoring attacks they are aligned [196, pp. 12–15, 19–20, 22, 25–27, 197–201].

In this simulation, the ICT PSP provider is a router provider based in a non-European Economic Area (EEA) nation state. The router provider sells routers to organisations in the EU internal market. The non-EEA nation state obtains remote administration specifications and credentials from the router provider that operate within the secure update mechanisms of the router. This allows the non-EEA nation state to monitor and control the router's data, services and functions in organisations in the EU internal market through remote administration functionality, which includes usage logging data management [50, 199]. The router is certified under an ECCS and, as such, meets the minimum security objectives.

Reconnaissance by the nation state identifies an organisation in the EU to target based on national interest. Nation state reconnaissance of the router was supplied by the router provider. The target organisation does not detect reconnaissance by the nation state. Weaponisation by the nation state involves obtaining up to date credentials for the remote administration functionality from the router provider and using an existing interest in a favourable territory external to the nation state from which to perform the attack [129, p. 206]. The organisation weaponises by using security by default in the router.

Delivery occurs when the target organisation puts the router into normal operation in the organisation. The nation state performs exploitation by entering valid remote administration credentials from the favourable territory, and with installation inherent to the remote administration functionality, the nation state obtains C&C in the form of the remote administration functionality within the existing secure update process. The nation state reviews router usage logging data and accesses organisation data in transit, removing entries from secure update usage logging data in the process. The organisation does not detect the activity as it is not monitoring the usage logging of the secure update process frequently. The organisation assumes it is a trusted process [50, 54, 112, p. 2].

Damage assessment, as well as the phases up to and including legal proceedings do not occur for the organisation as the attack is not detected by the organisation. Even if the organisation did detect the activity through secure update usage logging data monitoring, it may appear like normal secure update polling activity. Recovery would have no impact, as data was copied, not modified or deleted, and restoration of a previous router data image would merely restore the compromised secure update functionality with credentials that the router provider can provide to the nation state [1, Art. 51(h)]. Communication of the incident to the router provider would not be of assistance, as the router provider may explain the incident as inherent functionality

of the router to ensure secure updates are provided in a timely manner, and not as an attack [199]. Furthermore, if the router provider is required to provide a fix, such as by significantly limiting the remote administration functionality, the router provider may compromise the fix in another way, undetected by even their own designers and developers, to assist nation state monitoring and control [61, pp. 33–37].

In this simulation, the extent of collusion between the ICT PSP provider and the threat actor substantially undermines detection and denial by the target organisation. This simulation represents an extreme example of reconnaissance by a threat actor and the benefits it provides to the threat actor. This simulation also exemplifies the potential benefit in having security provided external to a certified ICT PSP to potentially mitigate against such collusion, limited by the extent to which that external provider is of interest to the nation state. Where the benefit of collusion is reduced by the use of external security measures, the nation state may instead rely on cyber espionage through new vulnerability identification, which may be similarly resistant to detection and denial by organisations, as illustrated in the cyber espionage simulation.

4.7 Conclusion

Qualitative simulation outcome analysis augments model analysis by providing practical context to further elucidate the outcome efficacy of the minimum security objectives.

The ransomware attack exemplified how social engineering can facilitate delivery, and how the outcome of the attack is primarily based on the strength of attacker reconnaissance as well as organisation use of least access privilege configuration and network segregation. It was recommended that the legal benefit of organisations using certified ICT PSPs be linked to organisations implementing least access privileges and network segregation for certified ICT PSPs.

The insider attack exemplified how physical security can be external to certified ICT PSPs, but is essential for their protection. It was recommended that the legal benefit of organisations using certified ICT PSPs be linked to the use of physical security measures around certified ICT PSPs.

The cyber espionage attack exemplified again how social engineering can facilitate delivery, even where security by default warns users, and again how the outcome of the attack is primarily based on the strength of attacker reconnaissance. The recommendation of regular training to limit social engineering, provided in model analysis, was reiterated to encourage users to act on security by default.

The hacktavist attack exemplified how attacks by less sophisticated threat actors that perform less reconnaissance on ICT PSPs and target organisations may be more easily detected and denied.

The nation state attack exemplified how extreme reconnaissance, through collusion with an ICT PSP provider, can result in attacks that are difficult to detect or deny.

In each simulation, attacker reconnaissance was determinative of the outcome, but was neither detected nor denied by the minimum security objectives. Detection and denial of the phases from delivery to action on objectives was primarily

provided by monitoring and acting upon usage logging data, while the strength of damage assessment, and hence communication, often depended on the availability and integrity of usage logging data. Recovery of data was generally not possible in the absence of external data retrieval, which is not explicitly permitted in the Cybersecurity Act. Evidence gathering, while supported by usage logging data, was not able to establish attacker identity, accentuating the importance of clarity on the admissibility and legal effect of evidence in the legal defence of organisations.

5 Conclusion

Legislative interpretation of the minimum security objectives illustrated the potential for significant diversity in interpretation. An attempt was made to provide clarity on the interpretation from the literal, systematic, functional, purposive and consequentialist perspectives. A clear understanding of what each of the objectives means at this early stage in the development of ECCSs is important in establishing their outcome efficacy.

Legislative interpretation did identify several gaps in the minimum security objectives that interpretive devices could not address, and recommendations were made with respect to each gap. The most remarkable gaps include: restorability does not extend to the full functionality of ICT PSPs, secure updates may contain known vulnerabilities and may create new vulnerabilities in ICT PSPs, and the minimum security objectives may not be operative during many phases of the lifecycle of certified ICT PSPs.

Model and simulation analysis revealed far more significant limitations in the outcome efficacy of the minimum security objectives than legislative interpretation alone. This is an important finding as it identifies model and simulation analysis as candidate analytic tools for assessment of the outcome efficacy of cybersecurity legislation. Indeed, both can be used in the process of drafting cybersecurity legislation.

Model analysis uncovered the majority of the observed limitations, compared to simulation analysis. Simulation analysis focused on specific attack scenarios, while model analysis was able to consider all attack scenarios. Simulation analysis, when combined with model analysis, added structure to the simulation and brought the limitations observed in model analysis into greater relief. Model analysis would be the first step in analysis, followed by combined simulation–model analysis to address specific scenarios of interest.

Turning to the limitations uncovered in model and simulation analysis, we see that attackers may engage in reconnaissance, weaponisation and delivery with little limitation. These phases are determinative to the outcome of attacks, and so we anticipate little improvement in the level of cybersecurity across the EU internal market with the minimum security objectives. There is also little attention to evidence gathering and legal proceedings, which, combined with little improvement in the level of cybersecurity, leaves organisations with no further opportunity to limit their losses from cyber attacks, which are likely to continue largely unabated.

The minimum security objectives are minimum objectives, and through the observations illustrated here and observations of others engaging in analysis of the minimum security objectives, ideally the limitations in the outcome efficacy of the minimum security objectives can be addressed. That is not sufficient, however, as it does not sufficiently address evidence gathering or legal proceedings. Ultimately there needs to be clarity at the EU level on evidence gathering and legal proceedings to provide a coherent functional legislative cybersecurity package that includes the GDPR, NIS Directive and Attacks Against Information Systems Directive, and to provide clear lines to organisations on how they may limit their losses from cyber attacks.

Acknowledgements doc. JUDr. Radim Polčák, Ph.D. for guidance and support; Katharina Margot Drescher, LL.M for support and review of drafts; Louis Ferguson, for support and review of drafts.

Funding This research was supported by the ERDF project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

Funding Open Access funding enabled and organized by Projekt DEAL.

Conflict of interest D. D. Stewart Ferguson declares that he has no competing interests.

References

1. European Union Agency for Cybersecurity (2019on) Regulation (EU) 2019/881 of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L151/15 (Cybersecurity Act). EU,
2. Leteinturier A et al Recommendations for the implementation of the CSP Certification scheme' (CSPCERT WG 2019). https://drive.google.com/file/d/1J2NJt-mk2iF_ewhPNnhTywpo0zOVcY8J/view. Accessed 13 Dec 2019
3. European Commission (2019) Towards a more secure and trusted cloud in Europe. https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe. Accessed 13 Dec 2019
4. ENISA (2020) Cybersecurity Certification. https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/. Accessed 8 Oct 2020
5. Raustiala K 'Compliance & Effectiveness in International Regulatory Cooperation' (2000) 32/3 Case W. Res. J. Int'l Law. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1497&context=jil. Accessed 2 Dec 2019 (387)
6. Postema GJ Conformity, Custom, and Congruence: Rethinking the Efficacy of Law' in MH Kramer, C Grant, B Colburn and A Hatzistavrou (eds), The Legacy of H.L.A. Hart: Legal, Political, and Moral Philosophy (Oxford University Press 2008). https://www.researchgate.net/publication/294113641_Conformity_Custom_and_Congruence_Rethinking_the_Efficacy_of_Law. Accessed 15 May 2020
7. Burazin L (2018) The concept of law and efficacy. https://www.researchgate.net/publication/317872826_The_Concept_of_Law_and_Efficacy. Accessed 3 Dec 2019
8. Coglianese C Measuring Regulatory Performance' (OECD 2012). https://www.oecd.org/gov/regulatory-policy/1_coglianese%20web.pdf. Accessed 3 Dec 2019

9. Itzcovich G (2009) 'The Interpretation of Community Law by the European Court of Justice' 10/5 German Law Journal. 537. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892093. Accessed 25 Sept 2019
10. Rösler H (2012) Interpretation of EU Law. In: Basedow J, Hopt KJ, Zimmermann R (eds) The Max Planck encyclopedia of European private law. Oxford University Press, Oxford (https://content.schweitzer-online.de/static/catalog_manager/live/media_files/representation/zd_std_orig__zd_schw_orig/001/136/708/9780199578955_content_pdf_1.pdf) accessed 23 September 2019)
11. Lenaerts K, Gutiérrez-Fons JA To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (European University Institute 2013). https://heinonline.org/HOL/LandingPage?handle=hein.journals/coljeul20&div=11&id=&page=. Accessed 24 Sept 2019
12. European Parliament Plenary Minutes. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html (Created 11 Mar 2019). Accessed 27 July 2019
13. Council of the European Union Council Minutes. https://www.consilium.europa.eu/register/en/content/out/?RESULTSET=1&DOC_SUBJECT=PV%20CONS&i=MING&ROWSPP=25&ORDERBY=ARCHIVEDATE%20DESC&DOC_LANCD=EN&typ=SET&NRROWS=500&DOC_YEAR=2019. Accessed 12 Dec 2019
14. EUR-Lex Procedure 2017/0225/COD. https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG. Accessed 27 July 2019
15. NIS Directive (2016) Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1
16. Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L26/48 (NIS Implementing Regulation).
17. Framework Directive (2002on) Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services [2002] OJ L108/33
18. Attacks Against Information Systems Directive (2013on) Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8
19. *Joined cases C-236/08 to C-238/08 Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08)* [2010] ECLI:EU:C:2010:159.
20. *Case C-324/09 L'Oréal SA and Others v eBay International AG and Others* [2011] ECLI:EU:C:2011:474.
21. *Case C-291/13 Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis* [2014] ECLI:EU:C:2014:2209.
22. Directive 2015/1535of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) [2015] OJ L241/1.
23. Mc Fadden T (2016) Case C-484/14 Tobias Mc Fadden v Sony Music Entertainment Germany GmbH [2016] ECLI:EU:C:2016:689
24. *Case C-434/15 Asociación Profesional Elite Taxi v Uber Systems Spain, SL* [2017] ECLI:EU:C:2017:981.
25. *Case C-320/16 Criminal proceedings against Uber France* [2018] ECLI:EU:C:2018:221.
26. Ellison RJ et al Evaluating and Mitigating Software Supply Chain Security Risks' (SEI Carnegie Mellon University 2010). https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15176.pdf. Accessed 17 Jan 2020
27. Miller JF 'Supply Chain Attack Framework and Attack Patterns' (MITRE 2013). https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf. Accessed 17 Jan 2020
28. Alberts C et al 'Assessing DoD System Acquisition Supply Chain Risk Management' (2017) 30/3 Cross Talk The Journal of Defense Software Engineering. 4. https://pdfs.semanticscholar.org/232e/d5c13b212b1ae98a6bf036c9a0a5b29437c3.pdf. Accessed 31 Dec 2019
29. National Counterintelligence and Security Center (2019) Supply chain risk management best practices. https://www.dni.gov/files/NCSC/documents/supplychain/20190405-UpdatedSCRM-Best-Practices.pdf. Accessed 18 Jan 2020

30. Regulation (EU) 2016/679 of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (GDPR).
31. Bensoussan A et al (2017) General Data Protection Regulation: texts, commentaries and practical guidelines. Wolters Kluwer,
32. Rücker D (2018) Scope of application of the GDPR. In: Rücker D, Kulger T (eds) New European General Data Protection Regulation A Practitioner's Guide. C.H. Beck Hart Nomos,
33. Schrey J (2018) General conditions for data processing in companies under the GDPR. In: Rücker D, Kluger T (eds) New European General Data Protection Regulation A Practitioner's Guide. C.H. Beck Hart Nomos,
34. Directive 2009/140/EC of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services [2009] OJ L337/37 (Framework Directive 2009).
35. eIDAS Regulation Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014) OJ L257/73
36. Directive (EU) (2018) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L321/36 (EECC)
37. UKICO (2019) Life at Parliament View Ltd
38. UKICO (2018) The Carphone Warehouse Limited
39. ECtHR (2008) I v. Finland App no 20511/03
40. UKICO (2018) Bupa Insurance Services Limited
41. CERT-EU Guidelines for handling common malware infections on Windows based workstations. https://media.cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_003_v2.pdf (Created 15 May 2012). Accessed 4 Jan 2020
42. U.S. DHS Alert (TA15-213A). https://www.us-cert.gov/ncas/alerts/TA15-213A (Created 29 Sept 2016). Accessed 11 Jan 2020
43. Le Jamtel E 'CERT-EU Security Whitepaper 17-004 Mitigating Risks Related to Network Devices' (CERT-EU 2017). https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_ND_17-004.pdf. Accessed 5 Jan 2020
44. Soria-Machado M et al 'CERT-EU Security Whitepaper 17-002 Detecting Lateral Movements in Windows Infrastructure' (CERT-EU 2017). https://cert.europa.eu/static/WhitePapers/CERT-EU_SWP_17-002_Lateral_Movements.pdf. Accessed 5 Jan 2020
45. U.S. DHS Alert (TA17-163A) CrashOverride Malware. https://www.us-cert.gov/ncas/alerts/TA17-163A (Created 27 July 2017). Accessed 11 Jan 2020
46. U.S. DHS Alert (TA17-164A) HIDDEN COBRA—North Korea's DDoS Botnet Infrastructure. https://www.us-cert.gov/ncas/alerts/TA17-164A (Created 23 Aug 2017). Accessed 4 Jan 2020
47. U.S. DHS Alert (TA17-318A) HIDDEN COBRA—North Korean Remote Administration Tool: FALLCHILL. https://www.us-cert.gov/ncas/alerts/TA17-318A (Created 22 Nov 2017). Accessed 11 Jan 2020
48. Flaglien AO (2018) The digital forensics process. In: Årnes A (ed) Digital forensics. John Wiley & Sons Ltd,
49. U.S. DHS Alert (TA17-293A) advanced persistent threat activity targeting energy and other critical infrastructure sectors. https://www.us-cert.gov/ncas/alerts/TA17-293A (Created 15 Mar 2018). Accessed 11 Jan 2020
50. U.S. DHS Alert (TA18-106A). https://www.us-cert.gov/ncas/alerts/TA18-106A (Created 20 Apr 2018). Accessed 11 Jan 2020
51. U.S. DHS Alert (TA18-276B) advanced persistent threat activity exploiting managed service providers. https://www.us-cert.gov/ncas/alerts/TA18-276B (Created 3 Oct 2018). Accessed 11 Jan 2020
52. U.S. DHS Alert (AA18-284A). https://www.us-cert.gov/ncas/alerts/AA18-284A (Created 11 Oct 2018). Accessed 11 Jan 2020
53. U.S. DHS Alert (AA18-337A). https://www.us-cert.gov/ncas/alerts/AA18-337A (Created 3 Dec 2018). Accessed 11 Jan 2020
54. U.S. DHS Alert (TA17-117A) intrusions affecting multiple victims across multiple sectors. https://www.us-cert.gov/ncas/alerts/TA17-117A (Created 20 Dec 2018). Accessed 11 Jan 2020
55. MS-ISAC Ryuk. https://www.cisecurity.org/wp-content/uploads/2020/01/Security-Primer-Ryuk.pdf (Created 20 Dec 2019). Accessed 11 Jan 2020

56. Otte L et al Comparison of Database Mirrors Technologies for Use in Fault-tolerant Information Systems Solutions' (2015 16th International Carpathian Control Conference (ICCC), Szilvasvarad, May 2015). https://www.researchgate.net/publication/308844853_Comparison_of_database_mirror_technologies_for_use_in_fault-tolerant_information_system_solutions. Accessed 15 Jan 2020
57. NIS Cooperation Group (2018) Reference document on security measures for Operators of Essential Services. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Accessed 11 Apr 2019
58. Ahmed E et al 'Seamless application execution in mobile cloud computing: Motivation, taxonomy, and open challenges' (2015) 52 Journal of Network and Computer Applications. 154. https://www.researchgate.net/publication/274320693_Seamless_application_execution_in_mobile_cloud_computing_Motivation_taxonomy_and_open_challenges. Accessed 15 Jan 2020
59. Cheraghlou MN, Khadem-Zadeh A, Haghparast M 'A survey of fault tolerance architecture in cloud computing' (2016) 61 Journal of Network and Computer Applications. 154. https://www.researchgate.net/publication/284069594_A_Survey_of_Fault_Tolerance_Architecture_in_Cloud_Computing. Accessed 14 Jan 2020
60. Dewar RS 'Active Cyber Defense, Cyber Defense Trend Analysis' (Center for Security Studies (CSS), ETH Zürich 2017). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-03.pdf. Accessed 7 Nov 2019
61. Lysne O (2018) The Huawei and Snowden Questions Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment? Springer, Cham (Aslak Tveito ed)
62. Biener C, Eling M, Wirfs JH 'Insurability of Cyber Risk: An Empirical Analysis' (2015) 40 The Geneva Papers, 131. https://www.researchgate.net/publication/265727415_Insurability_of_Cyber_Risk_An_Empirical_Analysis. Accessed 23 Oct 2019
63. Opinion of the European Economic and Social Committee COM(2017) 477 final/2 2017/0225 (COD) on the 'Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")' [2018] OJ C227/86.
64. NIS Cooperation Group (2018) Cybersecurity Incident Taxonomy. https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf. Accessed 4 Apr 2019
65. Katos V et al 'State of Vulnerabilities 2018–2019' (ENISA 2019). https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities. Accessed 15 Jan 2020
66. Karsberg C, Skouloudi C, Dekker M 'Annual Incident Reports 2013 Analysis of Article 13a annual incident reports' (ENISA 2014). https://www.enisa.europa.eu/publications/annual-incident-reports-2013. Accessed 16 Aug 2019
67. Karsberg C, Skouloudi C 'Annual Incident Reports 2014 Analysis of Article 13a annual incident reports' (ENISA 2015). https://www.enisa.europa.eu/publications/annual-incident-reports-2014. Accessed 16 Aug 2019
68. ENISA (2016) Annual Incident Reports 2015 Analysis of Article 13a annual incident reports in the telecom sector. https://www.enisa.europa.eu/publications/annual-incident-reports-2015. Accessed 16 Aug 2019
69. ENISA (2017) Annual Incident Reports 2016 Analysis of Article 13a annual incident reports in the telecom sector. https://www.enisa.europa.eu/publications/annual-incident-reports-2016. Accessed 16 Aug 2019
70. ENISA (2018) Annual Report Telecom Security Incidents 2017. https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017. Accessed 16 Aug 2019
71. Koukounas A, Vytogianni E, Dekker M 'Annual Report Telecom Security Incidents 2018' (ENISA 2019). https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2018. Accessed 16 Aug 2019
72. ENISA (2017) Annual Incident Analysis Report for the Trust Service Providers Analysis of Article 19a annual incident reports under eIDAS—2016. https://www.enisa.europa.eu/publications/annual-incident-analysis-report-for-the-trust-service-providers. Accessed 16 Aug 2019
73. ENISA (2018) Annual Report Trust Services Security Incidents 2017. https://www.enisa.europa.eu/publications/annual-report-trust-services-security-incidents-2017. Accessed 16 Aug 2019
74. Koukounas A, Vytogianni E, Dekker M 'Trust Services Security Incidents 2018 Annual Report' (ENISA 2019). https://www.enisa.europa.eu/publications/trust-services-security-incidents-2018. Accessed 16 Aug 2019

75. Symantec (2018) Internet Security Threat Report Volume 23. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf. Accessed 21 Apr 2019
76. ENISA (2017) ENISA Threat Landscape Report 2016 15 Top Cyber-Threats and Trends. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. Accessed 21 Feb 2019
77. ENISA (2018) ENISA Threat Landscape Report 2017 15 Top Cyber-Threats and Trends. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. Accessed 21 Feb 2019
78. Sfakianakis A et al 'ENISA Threat Landscape Report 2018 15 Top Cyber-Threats and Trends' (ENISA 2019). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018. Accessed 21 Feb 2019
79. Kott A (2014) 'Science of Cyber security as a system of models and problems. In: Robinson EP (ed) Network science and Cybersecurity. Springer, Berlin Heidelberg
80. Hubbard DW, Seiersen R (2016) How to measure anything in cybersecurity risk. John Wiley & Sons, Inc,
81. AL-Mohannadi H et al 'Cyber-Attack Modeling Analysis Techniques: An Overview' (4th International Conference on Future Internet of Things and Cloud Workshops, Vienna, August 2016). https://www.researchgate.net/publication/307174392_Cyber-Attack_Modeling_Analysis_Techniques_An_Overview. Accessed 15 July 2019
82. Couretas JM (2019) An introduction to cyber modeling and simulation. John Wiley & Sons, Inc,
83. Caltagirone S, Pendergast A (2013) The diamond model of intrusion analysis. http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf. Accessed 19 July 2019
84. Manadhata P, Wing JM 'An Attack Surface Metric' (2011) 37/3 IEEE Transactions on Software Engineering, 371. https://mlsec.info/pdf/tse11.pdf. Accessed 19 July 2019
85. Hutchins EM, Cloppert MJ, Amin RM 'Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains' (Lockheed Martin 2010). https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed 19 July 2019
86. 'APT1 Exposing One of China's Cyber Espionage Units' (Mandiant 2004). https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf. Accessed 18 July 2019
87. Cloppert M 'Security Intelligence: Attacking the Cyber Kill Chain' (SANS Digital Forensics and Incident Response Blog, 14 October 2009). https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain. Accessed 18 July 2019
88. Bodeau D, Graubart R (2013) 'Intended Effects of Cyber Resiliency Techniques on Adversary Activities' (2013 IEEE International Conference on Technologies for Homeland Security (HST). https://ieeexplore.ieee.org/document/6698967. Accessed 18 July 2019
89. Nachreiner C 'Kill Chain 3.0: Update the cyber kill chain for better defense' (Help Net Security, 10 February 2015). https://www.helpnetsecurity.com/2015/02/10/kill-chain-30-update-the-cyber-kill-chain-for-better-defense/. Accessed 17 July 2019
90. Malone ST 'Using an expanded cyber kill chain model to increase attack resiliency' (Black Hat USA 2016). https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf. Accessed 15 July 2019
91. Rutherford JR, White GB 'Using an Improved Cybersecurity Kill Chain to Develop an Improved Honey Community' (49th Hawaii International Conference on System Sciences, Koloa, 2016). https://ieeexplore.ieee.org/document/7427512. Accessed 16 July 2019
92. Laliberte M 'A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack' (Dark Reading, 21 September 2016). https://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952. Accessed 17 July 2019
93. Bryant BD, Saiedian H 'A novel kill-chain framework for remote security log analysis with SIEM software' (2017) 67 Computers & Security. 198. https://www.sciencedirect.com/science/article/pii/S0167404817300561. Accessed 18 July 2019
94. Pols P 'The Unified Kill Chain Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks' (MSc thesis, Leiden University 2017). https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf. Accessed 17 July 2019
95. Rege A et al 'A Temporal Assessment of Cyber Intrusion Chains Using Multidisciplinary Frameworks and Methodologies' (2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment, 2017). https://ieeexplore.ieee.org/document/8073398. Accessed 18 July 2019
96. Zhou X et al 'Kill Chain for Industrial Control System' (2018 International Conference on Smart Materials, Intelligent Manufacturing and Automation, Nanjing, 2018). https://www.matec-conferences.org/

articles/matecconf/abs/2018/32/matecconf_smima2018_01013/matecconf_smima2018_01013.html. Accessed 18 July 2019
97. Assante MJ, Lee RM 'The Industrial Control System Cyber Kill Chain' (SANS Institute 2019). https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297. Accessed 18 July 2019
98. Kim H, Kwon HJ, Kim KK 'Modified cyber kill chain model for multimedia service environments' (2019) 78/3 Multimedia Tools and Applications. 3153. https://link.springer.com/article/10.1007/s11042-018-5897-5. Accessed 15 July 2019
99. 'Enterprise Tactics' (MITRE). https://attack.mitre.org/tactics/enterprise/. Accessed 15 July 2019
100. 'Mobile Tactics' (MITRE). https://attack.mitre.org/tactics/mobile/. Accessed 15 July 2019
101. 'PRE-ATT&CK Tactics' (MITRE). https://attack.mitre.org/tactics/pre/. Accessed 15 July 2019
102. Harrington SL 'Cyber Security Active Defense: Playing with Fire or Sound Risk Management?' (2014) 10/4 Rich. J.L. & Tech. 1. https://scholarship.richmond.edu/jolt/vol20/iss4/2/. Accessed 11 Nov 2019
103. Craig AN, Shackelford SJ, Hiller JS 'Proactive Cybersecurity: A comparative industry and regulatory analysis' (2015) 52/4 American Business Law Journal. 721. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=257378. Accessed 7 Nov 2019
104. Cook C (2018) Cross-border data access and active cyber defense: assessing legislative options for a new international cybersecurity rulebook. Stan L Poly Rev 29:205
105. Heckman KE et al 'Denial and Deception in Cyber Defense' (2015) 48/4 Computer, 36. https://ieeexplore.ieee.org/abstract/document/7085646. Accessed 7 Nov 2019
106. UKICO (2018) Uber B.V., Uber London Limited, Uber Britannia Limited, Uber Scot Limited, Uber NIR Limited
107. UKICO (2017) Boomerang Video Ltd
108. 'Insider Threat Report' (Verizon 2019). https://enterprise.verizon.com/resources/reports/insider-threat-report/. Accessed 21 Apr 2019
109. UKICO (2018) University of Greenwich
110. Messier R (2017) Network forensics. John Wiley & Sons, Inc,
111. 'JexBoss—JBoss Verify and EXploitation Tool' (U.S. DHS, 8 November 2018). https://www.us-cert.gov/ncas/analysis-reports/AR18-312A. Accessed 4 Jan 2020
112. Boldea C-N, Socha K 'CERT-EU Security Whitepaper 2019-001 PowerShell—Cybersecurity Perspective' (CERT-EU 2019). https://media.cert.europa.eu/static/WhitePapers/CERT-EU-SWP2019-001.pdf. Accessed 5 Jan 2020
113. 'LockerGoga' (MS-ISAC, 28 March 2019). https://www.cisecurity.org/white-papers/security-primer-lockergoga/. Accessed 11 Jan 2020
114. Brandt A '"MegaCortex" ransomware wants to be The One' (Sophos News, 3 May 2019). https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/. Accessed 11 Jan 2020
115. 'Malware Analysis Report (AR19-304A) MAR-10135536-8—North Korean Trojan: HOPLIGHT' (U.S. DHS, 31 October 2019). https://www.us-cert.gov/ncas/analysis-reports/ar19-304a. Accessed 4 Jan 2020
116. Li Q, Clark G (2015) Security intelligence a practitioner's guide to solving enterprise security challenges. John Wiley & Sons, Inc,
117. Ghafir I et al Social engineering attack strategies and defence approaches. https://ieeexplore.ieee.org/document/7575856. Accessed 1 Jan 2020 (IEEE 4th International Conference on Future Internet of Things and Cloud, Vienna, August 2016)
118. Ariu D, Frumento E, Fumera G 'Social Engineering 2.0: A Foundational Work' (Computing Frontiers, Siena, May 2017). https://www.doganaproject.eu/images/PDF_Files/ComputingFrontiers17_DAriu_final_.pdf. Accessed 1 Jan 2020
119. DiMaggio J The Black Vine cyberespionage group. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf. Accessed 4 Jan 2020 (Symantec, 2015)
120. Silfversten E et al Economics of vulnerability disclosure. https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure. Accessed 27 Sept 2019 (ENISA 2018)
121. UKICO (2018) Equifax Ltd
122. Kaspersky Availability of Documentation. https://www.kaspersky.com/resource-center/threats/malware-documentation. Accessed 4 Jan 2020
123. Conteh NY, Schmick PJ (2016) Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks, 31. Int J Adv Comput Res 6(23):31. https://doi.org/10.19101/IJACR.2016.623006

124. Kosseff J 'Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System' (2016) 19/2 Chap. L. Rev. 401. http://digitalcommons.chapman.edu/chapman-law-review/vol19/iss2/3. Accessed 13 Dec 2019
125. Norvanto E (2018) The human layer of cybersecurity—the art of social engineering. In: Rehrl J (ed) Handbook on Cybersecurity The Common Security and Defence Policy of the European Union, vol 5. Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria,
126. Kaplan JM et al (2015) Beyond Cybersecurity Protecting your digital business. John Wiley & Sons, Inc, and others
127. Messer A, Medairy B (2018) The future of cyber defense... going on the offensive. Cyber Def Rev 3(3):37
128. Plohmann D, Gerhards-Padilla E, Leder F Botnets: Detection, Measurement, Disinfection & Defence. https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence. Accessed 8 July 2019 (Giles Hogben ed, ENISA 2011)
129. Wangen G (2015) 'The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism' 6 Information, 183. https://res.mdpi.com/d_attachment/information/information-06-00183/article_deploy/information-06-00183.pdf. Accessed 8 Nov 2019
130. 'Regin: Top-tier espionage tool enables stealthy surveillance' (Symantec, 27 August 2015). https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf. Accessed 4 Jan 2020
131. 'Malware Analysis Report (AR18-165A)' (U.S. DHS, 14 March 2019). https://www.us-cert.gov/ncas/analysis-reports/AR18-165A. Accessed 4 Jan 2020
132. 'Malware Analysis Report (AR19-252A)' (U.S. DHS, 9 September 2019). https://www.us-cert.gov/ncas/analysis-reports/ar19-252a. Accessed 4 Jan 2020
133. Montagnani ML, Cavallo MA 'Cybersecurity and Liability in a Big Data World' (2018) 2/2 Market and Competition Law Review. 71. https://www.researchgate.net/publication/336658024_Cybersecurity_and_Liability_in_a_Big_Data_World. Accessed 13 Dec 2019
134. Sunde IM (2018) Cybercrime Law. In: Årnes A (ed) Digital Forensics. John Wiley & Sons Ltd,
135. 'Electronic evidence—a basic guide for First Responders' (ENISA 2014). https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders. Accessed 27 Sept 2019
136. Dilijonaite A (2018) Digital forensic readiness. In: Årnes A (ed) Digital forensics. John Wiley & Sons Ltd,
137. Marcella AJ Jr., Guillossou F (2012) Cyber forensics from data to digital evidence. John Wiley & Sons Ltd,
138. Årnes A (2018) Introduction. In: Årnes A (ed) Digital forensics. John Wiley & Sons Ltd,
139. Laykin E (2013) Investigative computer forensics. John Wiley & Sons, Inc,
140. Boldea C, Antoniou D 'Data Acquisition Guidelines for Investigation Purposes' (CERT-EU 2019). https://media.cert.europa.eu/static/WhitePapers/CERT-EU-SWP2012-004.pdf. Accessed 5 Jan 2020
141. Stevens R, Biller J 'Offensive Digital Countermeasures: Exploring the Implications for Governments' (2018) 3/3 The Cyber Defense Review, 93. https://www.jstor.org/stable/26555000?seq=1#metadata_info_tab_contents. Accessed 20 Nov 2019
142. Roman J 'DDoS Response: Communication Tips' (BankInfoSecurity, 31 October 2002). https://www.bankinfosecurity.com/ddos-response-communication-tips-a-5250. Accessed 18 Jan 2020
143. Savage K, Coogan P, Lau H 'The evolution of ransomware' (Symantec 2015). https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf. Accessed 4 Jan 2020
144. NIS Cooperation Group (2018) Guidelines on notification of Digital Service Providers incidents Formats and procedures. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Accessed 4 Apr 2019
145. NIS Cooperation Group (2018) Guidelines on notification of Operators of Essential Services incidents Formats and procedures. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Accessed 4 Apr 2019
146. NIS Cooperation Group (2018) Reference document on Incident Notification for Operators of Essential Services Circumstances of notification. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Accessed 4 Apr 2019
147. 'State of Software Security' (Volume 10, Veracode 2019). https://www.veracode.com/sites/default/files/pdf/resources/sossreports/state-of-software-security-volume-10-veracode-report.pdf. Accessed 11 Dec 2019

148. Marinos L, Sfakianakis A ENISA Threat Landscape Responding to the Evolving Threat Environment' (ENISA 2012). https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape. Accessed 21 Feb 2019
149. Marinos L, Sfakianakis A 'ENISA Threat Landscape 2013 Overview of current and emerging cyber-threats' (ENISA 2013). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats. Accessed 21 Feb 2019
150. Marinos L, Sfakianakis A 'ENISA Threat Landscape 2014 Overview of current and emerging cyber-threats' (ENISA 2014). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014. Accessed 21 Feb 2019
151. Marinos L, Sfakianakis A, Belmonte A, Rekleitis E 'ENISA Threat Landscape 2015' (ENISA 2016). https://www.enisa.europa.eu/publications/etl2015. Accessed 21 Feb 2019
152. ECSO (2017) Strategic Research and Innovation Agenda. https://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf. Accessed 7 Apr 2019
153. Zrahia A (2018) Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. J Cybersecur 1:1–16. https://doi.org/10.1093/cybsec/tyy008
154. 'Alert (TA17-181A)' (U.S. DHS, 15 February 2018). https://www.us-cert.gov/ncas/alerts/TA17-181A. Accessed 4 Jan 2020
155. ENISA (2015) CERT Capability team, 'Good Practice Guide on Vulnerability Disclosure. https://www.enisa.europa.eu/publications/vulnerability-disclosure. Accessed 30 July 2019
156. Lin H 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (Hoover Institution 2016). https://www.hoover.org/research/attribution-malicious-cyber-incidents-soup-nuts-0. Accessed 11 Nov 2019
157. Mueller M et al 'Cyber Attribution' (2019) 4/1 The Cyber Defense Review, 107. https://www.jstor.org/stable/26623070?seq=1#metadata_info_tab_contents. Accessed 20 Nov 2019
158. Dekker M, Karsberg C, Moulinos K 'Security framework for Article 4 and 13a' (ENISA 2013). https://www.enisa.europa.eu/publications/proposal-for-one-security-framework-for-articles-4-and-13a. Accessed 30 July 2019
159. Dekker M, Karsberg C 'Technical Guideline on Security Measures' (ENISA 2014). https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf. Accessed 30 July 2019
160. ENISA (2018) Guidelines on assessing DSP and OES compliance to the NISD security requirements. https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements. Accessed 30 June 2019
161. UKICO (2018) Heathrow airport limited
162. ENISA (2016) Cyber insurance: recent advances, good practices and challenges. https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges. Accessed 8 July 2019
163. Baban CP et al 'Cyber Insurance as a Contribution to IT Risk Management. An Analysis of the Market for Cyber Insurance in Germany' (Brandenburg Institute for Society and Security 2017). https://www.bigs-potsdam.org/images/PP_No7_Cyber%20Insurance.pdf. Accessed 23 Oct 2019
164. Marotta A et al (2017) Cyber-insurance survey. Comput Sci Rev 24:35
165. Romanosky S et al (2019) Content analysis of cyber insurance policies: how do carriers price cyber risk? J Cybersecur 5(1):1
166. CHUBB (2016) Terms and Conditions Cyber Enterprise Risk Management Insurance. https://www.chubb.com/cz-cz/_assets/documents/chubb_pp-cyber-enterprise-risk-management-en.pdf. Accessed 10 Dec 2019
167. Kosseff J (2017) Cybersecurity law. John Wiley & Sons, Inc,
168. Lindsay N 'Businesses Are Finding Out That Cyber Insurance Coverage Might Not Be What They Thought' CPO Magazine (Singapore, 31 January 2019). https://www.cpomagazine.com/cyber-security/businesses-are-finding-out-that-cyber-insurance-coverage-might-not-be-what-they-thought/. Accessed 9 Dec 2019
169. Satariano A, Perlroth N 'Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong' New York Times (New York City, 15 April 2019). https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html. Accessed 6 Dec 2019
170. Hiller JS 'Civil Cyberconflict: Microsoft, Cybercrime, and Botnets' (2014) 31/2 Santa Clara High Tech L.J, 163. https://pdfs.semanticscholar.org/cfe1/4fd54a19c0ac1e3b0869104681adfb4a1363.pdf. Accessed 5 Dec 2019
171. Lerner Z 'Microsoft The Botnet Hunter: The Role of Public-Private Partnerships In Mitigating Botnets' (2014) 28/1 Harvard Journal of Law & Technology, 237. http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech237.pdf. Accessed 5 Dec 2019

172. Directive 2000/31/EC of 8 June 2000on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1 (eCommerce Directive).
173. *Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECLI:EU:C:2011:771.
174. Directive (EU) 2016/943 of 8 June 2016on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1 (Trade Secrets Directive).
175. Deem M (2018) Liability following a data breach. In: Wong H (ed) Cybersecurity: law and guidance. Bloomsbury Professional,
176. Lorimer J, Christopher W (2018) Criminal law. In: Wong H (ed) Cybersecurity: law and guidance. Bloomsbury Professional,
177. Protocol No. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms (22 November 1984, entered into force 1 November 1988) ETS No.117.
178. Regulation (EU) No 1215/2012of 12 December 2012on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1.
179. Directorate of the Jurisconsult 'Guide on Article 4 of Protocol No. 7 to the European Convention on Human Rights: Right not to be tried or punished twice' (ECtHR 2019). https://www.echr.coe.int/Documents/Guide_Art_4_Protocol_7_ENG.pdf. Accessed 2 Dec 2019
180. *Case C-47/18 Skarb Pánstwa Rzeczpospolitej Polskiej—Generalny Dyrektor Dróg Krajowych i Autostrad v Stephan Riel* [2019] ECLI:EU:C:2019:754.
181. Regulation (EU) No 526/2013of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 [2013] OJ L165/41.
182. MITRE Common weakness enumeration. https://cwe.mitre.org/data/index.html. Accessed 10 May 2019
183. NIST National vulnerability database. https://nvd.nist.gov. Accessed 8 Apr 2019
184. U.S. DHS (2018) Alert (TA17-132A) indicators associated with wannacry ransomware. https://www.us-cert.gov/ncas/alerts/TA17-132A. Accessed 4 Jan 2020
185. UKICO (2018) The British and foreign bible society
186. Europol No More Ransom Update: Belgian Federal Police Releases Free Decryption Keys for the Cryakl Ransomware. https://www.europol.europa.eu/newsroom/news/no-more-ransom-update-belgian-federal-police-releases-free-decryption-keys-for-cryakl-ransomware (Created 9 Feb 2018). Accessed 12 Mar 2019
187. Europol Pay No More: Universal GandCrab Decryption Tool Released for Free on No More Ransom. https://www.europol.europa.eu/newsroom/news/pay-no-more-universal-gandcrab-decryption-tool-released-for-free-no-more-ransom (Created 25 Oct 2018). Accessed 12 Mar 2019
188. No More Ransom No more ransom! https://www.nomoreransom.org/en/index.html. Accessed 12 Mar 2019
189. Cybersecurity Insiders (2018) Insider Threat 2018 Report. https://www.cybersecurity-insiders.com/download-reports/. Accessed 1 May 2019
190. Trend Micro Trend micro discloses insider threat impacting some of its consumer customers. https://blog.trendmicro.com/trend-micro-discloses-insider-threat-impacting-some-of-its-consumer-customers/ (Created 5 Nov 2019). Accessed 8 Jan 2020
191. Schwartz A (2015) The Exclusiveness of Malicious Software Called Spyware and Exploring Mitigating Techniques. Natl Cybersecur Inst J 2(1):51
192. Kara İ, Aydos M 'The Ghost in the System: Technical Analysis of Remote Access Trojan' (2019) 11/1 IJITS, 73. https://ijits-bg.com/contents/IJITS-No1-2019/2019-N1-08.pdf. Accessed 30 Dec 2019
193. Vance A (2017) What do we really know about how habituation to warnings occurs over time?: a longitudinal fMRI study of habituation and polymorphic warnings. CHI Conference on Human Factors in Computing Systems, Denver, 05.2017. https://doi.org/10.1145/3025453.3025896
194. 'SQL Injection' (MS-ISAC, 20 May 2017). https://www.cisecurity.org/wp-content/uploads/2017/05/SQL-Injection-White-Paper2.pdf. Accessed 11 Jan 2020
195. Revuelto V, Meintanis S, Socha K 'CERT-EU Security Whitepaper 17-003 DDoS Overview and Response Guide' (CERT-EU 2017). https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf. Accessed 5 Jan 2020
196. NIS Cooperation Group (2019) EU coordinated risk assessment of the cybersecurity of 5G networks. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132. Accessed 13 Dec 2019

197. McCarthy T 'NSA director defends plan to maintain 'backdoors' into technology companies' The Guardian (London, 25 February 2015). https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies. Accessed 7 Dec 2019
198. Whittaker Z 'Tech giants hit by NSA spying slam encryption backdoors' ZDNet (2 May 2018). https://www.zdnet.com/article/coalition-of-tech-giants-hit-by-nsa-spying-slams-encryption-backdoors/. Accessed 7 Dec 2019
199. Neate R 'Huawei says alleged router 'backdoor' is standard network tool' The Guardian (London, 30 April 2019). https://www.theguardian.com/technology/2019/apr/30/alleged-huawei-router-backdoor-is-standard-networking-tool-says-firm. Accessed 9 Dec 2019
200. Tung L 'Huawei security: Half its kit has 'at least one potential backdoor" ZDNet (27 June 2019). https://www.zdnet.com/article/huawei-security-half-its-kit-has-at-least-one-potential-backdoor/. Accessed 07.12.
201. Kaska K, Beckvard B, Minárik T 'Huawei, 5G and China as a Security Threat' (CCDCOE, 2019). https://www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf#page10. Accessed 9 Dec 2019
202. Hamm J (2018) 'Computer Forensics' in André Årnes (ed) Digital Forensics. John Wiley & Sons Ltd.

Donald David Stewart Ferguson PhD student at the University of Göttingen, Niedersachsen, Germany