Denying the Deniers:

A Comparative Case Study of the Dutch and American Approaches to DDoS Deterrence

Author:	Matej Dolinsek
Student Number:	S1567837
Thesis Supervisor:	Dr. Tommy van Steen
Second Reader:	Dr. Joery Matthys
Program:	MSc Crisis and Security Management
Date of Submission:	16.01.2021
Word Count:	23,860

Table of Contents

LIST OF ABBREVIATIONS

Technical Abbreviations:

DDoS	Distributed Denial of Service
DoS	Denial of Service
NBIP	*Nationale Beheersorganisatie Internet Providers*
SIDN	*Stichting Internet Domeinregistratie Nederland*
CSP	Cloud Service Provider
DSP	Digital Service Provider
SaaS	Software as a Service
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
DMZ	Demilitarized Zone
VMM	Virtual Machine Monitor
VM	Virtual Machine
PC	Personal Computer
QoS	Quality of Service
IP	Internet Protocol
TCP	Transmission Control Protocol
DHCP	Dynamic Host Configuration Protocol
NAT	Network Address Translation
PHI	Protected Health Information
PII	Personally Identifiable Information
NFR	Non-Functional Requirement
IETF	Internet Engineering Task Force
DiD	Defence-in-Depth
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SIEM	Security Information and Event Management
RBAC	Role-Based Access Control

Legislative Abbreviations:

HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
FISMA	Federal Information Security Modernization Act
GDPR	General Data Protection Regulation
NIS	Network and Information Systems Directive
Wbni	Network and Information Security Act (*Wet beveiliging netwerk- en informatiebeveiliging)*
SOX	Sarbanes-Oxley Act

Vibr	Information Security for the National Services Decree (*Voorschrijft Informatiebeveiliging Rijksdienst*)
Vibr-Bi	Information Security for the National Services Decree – Special Information (*Voorschrijft Informatiebeveiliging Rijksdienst – Bijzondere Informatie*)
Av	Archive Law (*Archiefwet*)
Wvo	Security Investigations Act (*Wet veiligheidsonderzoeken)*
Tw	Telecommunications Act (*Telecommunicatiewet)*
Wc	Computer Criminality Act (*Wet Computercriminaliteit)*
Wob	Government Information – Public Access Act (*Wet Openbaarheid van Bestuur)*
Webv	Administrative Electronic Traffic Act (*Wet Elektronisch Bestuurlijk Verkeer)*

Organizational Abbreviations:

ENISA	European Network and Information Security Agency
CISA	United States Cyber security and Infrastructure Security Agency
HHS	United States Department of Health and Human Services
OMB	United States Office of Management and Budget
NSC	United States National Security Council
DHS	United States Department of Homeland Security
GSA	United States General Services Administration
NIST	National Institute of Standards and Technology
FBI	United States Federal Bureau of Investigation
AP	Netherlands Data Protection Authority (*Autoriteit Persoonsgegevens*)
EZK	Netherlands Ministry for Economic Affairs and Climate Policy
NCSC	Netherlands National Cyber Security Centre
ISO	International Organization for Standardization
FedRAMP	Federal Risk and Authorization Management Program

1.0 INTRODUCTION

During the course of the last decade, DDoS attacks have become increasingly more commonplace in the Netherlands. It is on a regular basis that the Dutch public is faced with news concerning various forms of DDoS attacks having occurred against, among others, the Dutch Tax and Customs Administration (*Belastingdienst*)[1], the digital identity management system (*DigiD*)[2], banks and financial institutions[3], as well as schools and educational institutions[4], to name but a few. The Dutch National Internet Providers Management Organization (NBIP) estimates that in 2019 on average 2.5 DDoS attacks occurred against .nl registered domains every day, making Dutch private and public sector organizations, as well as the citizenry as a whole, no strangers to such attacks (de Weerdt et al. 2020, p.11). Furthermore, studies have shown the Netherlands to be a considerable outlier in terms of the number of DDoS attacks that originate from its jurisdiction, as for multiple consecutive periods within the last decade the country ranked third highest in the world by the aggregate number of outgoing DDoS attacks, eclipsed only by cyber giants the likes of Russia and the USA (McKeay et al. 2019a, p. 20-21; Overvest and Straathof 2015, p. 9). Recent studies conducted by the Dutch Internet Domain Registration Organization (SIDN) indicate that such incidents of varied severity have been reported by approximately 42%, thus almost half of all large enterprises and organization with 250+ employees and are also not foreign to small and medium sized enterprises as well (Boerman et al. 2018, p. 12). Striking statistics, such as that the largest DDoS attack recorded in the Netherlands in 2017 (36 Gbps) would not have even made the list of top 10 largest attacks in 2018 and 2019, permeate the Internet and security community creating a grave sense of urgency regarding this subject area (de Weerdt et al. 2020, p. 23).

While cyber incidents of all kinds are becoming increasingly commonplace occurrences in today's digitalized environment, the contextual factors within which they are taking place should not be extricated from the equation. Particularly with DDoS attacks, and perhaps more so than with any other type of cyber-attack, the attack's ramifications are felt by a plurality of actors that share the common logical and technological space that we call the Internet. Studies have found that, contrary to what one might first imagine, for the majority of companies and organizations "the probability of suffering collateral DDoS damage is significantly higher than the probability of being the intended target" (Boerman et al. 2018, p.18). Moving up a level of abstraction, the problem of collateral damage becomes even more significant when observed within the context of an increasing centrally collocated, cloud-based Internet environment. Virtualization and cloud native technologies such as containers are changing notions of utility computing and as a result also influencing the way DDoS attacks impact the Internet and its users, as well as by extension, how such attacks can be mitigated. The last decade in particular has witnessed

[1] DDoS-aanval belasting en douane [DDoS attack on tax and customs authorities], NOS.nl, 10-05-2019. https://nos.nl/artikel/505247-ddosaanval-belasting-en-douane.html

[2] Kort problemen met website DigiD door DDoS-aanval [Brief problems with DigiD website due to DDoS attack], NOS.nl, 31-07-2018. https://nos.nl/artikel/2244007-kort-problemen-met-website-digid-door-ddos-aanval.html

[3] Banken waren opnieuw doelwit van ddos-aanval [Banks targeted by another DDoS attack], Tweakers 28-05-2018 https://tweakers.net/nieuws/139053/banken-waren-opnieuw-doelwit-van-ddos-aanval.html

[4] Radboud Universiteit vijf keer doelwit ddos-aanval, gelast tentamen af [Radboud University targeted five times by DDoS Attacks, cancels exams], NU.nl, 07-12-2019 https://www.nu.nl/tech/6016132/radboud-universiteit-vijf-keer-doelwit-ddos-aanval-gelast-tentamen-af.html

many governments and industries migrate their traditional IT infrastructure into the Cloud, powered by the widespread adoption of virtualization technologies and the flexible cloud computing service models being offered by Cloud Services Providers (CSP) (Somani et al. 2017, p.30; Subramanian and Jeyaraj 2018, p.28). These include PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and SaaS (Software as a Service) (Subramanian and Jeyaraj 2018, p.28). The large data centres and data processing facilities required for running these virtualized environments form the backbone of many commercial, social, and industrial activities, making their disruption costly as well as the resultant damage distributed across multiple entities that make use of the shared hosting environment (European Commission 2012, p.4). These factors are leading to DDoS attacks increasingly becoming the tool of choice for a number of parties aiming to cause disruption. Incidentally, the aims and aspirations of these parties could hardly be further removed from each other and are often understudied and overshadowed by more visible threats such as cyber warfare (Wilner 2020, p.256).

In order to continue to confront these issues, the academic discipline of criminology must increasingly reach out into the fields of science and technology to sufficiently grasp at the problem area and establish effective methods for deterring this contemporary, technologically driven, anti-social behaviour. Given the fast-paced advancement of computing technologies however, this is certainly no easy feat. Due to their ability to leverage know-how, standardization, and form better economies of scale, virtualized/cloud environments (logical layer) and their data centre counterparts (physical layer) are enabling the propagation of cheap, more efficient, and more accessible utility computing, served on demand globally to anyone with an Internet connection (European Commission 2012, p.4). Their ability to leverage and improve the consumption of limited resources required for the continued functioning of the Internet also inadvertently puts them at the forefront of defensive efforts in cases of resource exhaustion attacks, such as DDoS. Overemphasis on the role of states and high-end cyber threats has led many studies to favour policy prescription over more theoretical, methodological and empirical research approaches, creating a gap in this field of study (Wilner 2020, p.256). Overly prescriptive approaches have also resulted in research often measuring spurious relationships, such as that between cyber-attacks and financial loss, as opposed to studying the interplay between technical, environmental and other relevant factors and variables that could potentially have a dissuading effect on this sort of crime. In the context of DDoS, these could include but are certainly not limited to availability requirements and service-level agreements (SLAs), which play a more important and direct role in impact and recovery than revenue (see also Boerman et al. 2018, p.15; Overvest & Straathof 2015, p.2).

The aim of this research paper is therefore to lessen the analytical ambiguity of existing cyber criminology studies by examining a specific, highly prevalent form of cybercrime within a particular technological context of virtualized computing. Due to the diversity of actors and motivations within this space, the level of analysis does not focus on the cybercriminals and crime propagators, but rather examines how the technology of the day can be leveraged to deter such criminal behaviour and ameliorate its effects. Traditional criminological theory puts considerable emphasis on the punishment of criminals, however seeing as how traditional forms of crime prevention are ineffective in most cybercrime contexts, means of prevention must necessarily look to information security to establish preventive methods. In this regard, criminological deterrence by denial consisting of resilience and resistance factors, as developed by criminological studies in the 20th century, is becoming ever more pertinent to the current digitalized context. The following research paper will thus examine the applicability of the theory of criminological deterrence in cyberspace by applying the theory to a comparative case study, comparing legislation in the U.S. and the Netherlands. The case study design will examine the information security resistance and resilience strengthening practices associated with controlling the Internet design flaws that permit the technological feat of DDoS attacks, and the extent to which legislation in both case countries requires the implementation of said controls to mitigate these known issues.

1.1 Research Question:

To what extent are Dutch and American cloud services providers and other entities hosting virtualized computing environments obliged by legislation to implement resistance and resilience strategies that mitigate the DDoS enabling design aspects of the Internet?

2.0 THEORETICAL FRAMEWORK

2.1 Evolution of Deterrence Theory:

Deterrence theory has featured prominently in a number of fields of academic study, including psychology, sociology, international relations, and criminology. Tracing its roots to utilitarian philosophy and initially put forward by Jeremy Bentham (1748-1832) and Cesare Beccaria (1738-1794) in the 18th century, the underlying premise of deterrence theory postulated individuals as rational actors who will commit crimes if these will provide a net positive outcome (Siponen and Vance 2010, p.491). In viewing individuals as rational actors, any commissioning of a crime would inevitably be preceded by a rational calculation of whether the costs of committing the crime would exceed the benefits (Kennedy 1983, p.2). In other words, criminals will commit a crime "when it pays" (Siponen and Vance 2010, p.491). Criminal deterrence is traditionally considered to have two dimensions, the preventive and deterrent (Kennedy 1983, p.1). The preventive dimension is defined as follows:

> *"In the broad usage, a deterrent is anything which exerts a preventive force against crime. Usually, but not necessarily, we are interested in the preventive effects of crime control measures which are introduced by law enforcement agencies"* (Kennedy 1983, p.1)

The deterrent dimension on the other hand, is defined as the:

> *"Control or alteration of present and future criminal behaviour which is effected by fear of adverse extrinsic consequences resulting from that behaviour. This dimension is, in essence, the deliberate threat of harm, communicated to the public generally, to discourage socially proscribed conduct across all society"* (Kennedy 1983, p.2).

In this context, Bentham and Beccaria initially proposed certainty, severity and celerity of punishment as the variables inversely affecting the rate of commission of a particular criminal offense (Akers 1990, p.660; Kennedy 1983, p. 4). A rational individual considering the commission of a criminal offense will thus assume the risk of getting apprehended (certainty of sanctions), the risk of incurring the penalties defined for that particular offense (severity of sanctions) and the risk of incurring these penalties immediately or soon after committing the offense (celerity of sanctions) (Siponen and Vance 2010, p. 491). If assuming these risks outweighs the benefits of reward committing the offense will provide the individual, he or she will be deterred from committing the crime.

2.1.1 Three 'Waves' of Deterrence Theory:

With the advent of the nuclear age, deterrence theory came to be featured prominently in International Relations academia, including security studies, as a result of the Cold War stand-off between the two superpowers, the USSR and the USA (Benediek and Metzger 2015, p.555; Akers 1990, p. 654; Knopf 2010, p.1). Robert Jervis in his work outlined three "waves" of deterrence theorizing, which led to the development of new deterrence variables (Brantly 2018, p.33; Knopf 2010, p.1). At the time of the high Cold War, the geopolitical context led scholars to develop two new deterrence variables, including credibility and signalling (Benediek and Metzger 2015, p. 555). Credibility requires an actor to be ready to defend their interests, as well to have the ability to defend those interests, while signalling is the notion that an actor requires to both communicate those interests to potential transgressors, as well as the threats that are to materialize in the case of a transgression (Benediek and Metzger 2015, p.555). Apart from deterrence by punishment (or retaliation, depending on the context), this era saw the development of another domain that became known as 'deterrence by denial', with 'deterrence by resistance' and 'deterrence by resilience' becoming two separate approaches within this domain (Benediek and Metzger 2015, p. 557). The intention behind both of these two approaches is to nullify a transgressor's gains, the prior by creating impregnable defences that would be too difficult to overcome, and the latter by recovering from an attack with enough efficiency as to offset any potential gains made by the opposing party (Benediek and Metzger 2015, p. 557). Theoretical development in subsequent years also saw the emergence of deterrence concepts that were more critical of the "rigorous concepts of rationality" common across the deterrence disciplines (Brantly 2018, p.33; Benediek and Metzger 2015, p. 556).

In recent decades however, the intense scholarship on the topic of deterrence has created variations in the deterrence variables, as the theory was extended and modified to accommodate particular fields, including that of cyber security (Siponen and Vance 2010, p. 491). In spilling over into other disciplines, academics have tried to limit the bias towards legal reinforcement by expanding the theory to go beyond the mere risk of legal sanction and include a more holistic behavioural formula that includes both positive and negative punishment and reinforcement, as well as a range of variables influencing both criminal and conforming behaviour (Akers 1990, p.660).

2.2 Theoretisizing Deterrence in Cyberspace:

One of these other disciplines also includes the relatively nascent cyber domain, as academics continue to map the various characteristics and unique problems of this vast landscape in order to understand the decision making processes of its many decentralized and varied participants (Wilner 2020, p. 251). The *en masse* global adoption of computing tools and resources, as well as the transposition of communities and social networks into virtual spaces required a re-conceptualization of the characteristics which underline these social interactions. In more technical terms, there is a continuous increase in the aggregate number of untrusted nodes that wish to communicate over the network, which is effectively changing notions of trust, participant relationships, and influencing decision making processes as a result (Cooper 2012, p.106; Brantly 2018, p.39; Blumenthal and Clark 2001, p. 93). The cyber domain represents not only a virtual operational space with unique interactions, risks, rewards, and other distinct characteristics, but is marked by an increasing abstraction and reliance on the availability of computing resources that is influencing the way we not only interact with each other, but also the way we interact with machines (Cooper 2012, p.106; Brantly 2018, p.39; Sigholm 2016, p.2).

Traditional security and cybercrime deterrence models focusing on binary defence concepts such as the DMZ (trusted vs. untrusted boundary) are no longer suitable in providing security in such abstracted, contemporary networks that are characterized by highly available and dynamic environments (DeCusatis et al. 2016, p. 5). The traditional 'implicit trust' security model (also known as the "trust but verify" approach) focuses on enforcing defences at the network boundary by verifying whether the requestor and receiver both belong to a particular trusted security group or domain, and should therefore be allowed to communicate (DeCusatis et al. 2016, p.5). However, in light of widespread cloud computing, resource sharing (e.g. VMM) and hybrid partitioning of network architectures (e.g. partly on-premise, partly in the cloud), the notion of a strict network boundary separating the trusted and untrusted realms is quickly becoming obsolete (DeCusatis et al. 2016, p.5). Already in 2001, Blumenthal and Clark stated that "of all the changes that are transforming the Internet, the loss of trust may be the most fundamental… The simple model of the early Internet—a group of mutually trusting users attached to a transparent network—is gone forever" (2001, p.93). Instead, contemporary networks are increasingly pushing the adoption of a 'zero-trust' model (also known as the "trust nothing, verify everything" approach), which stipulates that all traffic should be monitored and validated, regardless of source or destination (DeCusatis et al. 2016, p.6). Such an approach is more suitable to support other security concepts such as defence-in-depth and could in theory be layered to the extent of authenticating individual packets themselves (DeCusatis et al. 2016, p.6).

Brantly's characterization of the interaction of the virtual and physical realms, far from being limited only to infrastructure, is demonstrated in everyday reliance on essential digital services to complete, potentially critical, physical tasks. The contemporary level of human-machine interaction implies that far from only changing human norms and relationships, the demands to increase participation rates and lower the barriers of access to 'on demand' computer services, is also changing the way that technology is developing to face these challenges. In an effort to meet requirements, the custodians of large, global computer infrastructures, including data centres and other service providers, focus on optimizing their networks "to provide high throughput, low latency and high availability" (Govindan et al. 2016, p. 58). Considering that issues with a single device can potentially bring down or degrade the functioning of a network, designing networks of such scale and heterogeneity presents administrators and engineers with significant problems (Govindan et al. 2016, p. 58). For example, fast-paced rolling out of new services and adapting to the elasticity in traffic demand means that the velocity of evolution of such networks is significant, posing challenges such as complexity management, traffic congestion, or shortages of qualified personnel, to name but a few (Govindan et al. 2016, p. 58). Nevertheless, tenants who are hosted in these environments often times expect the services that they are running to be available "at any time and accessible from anywhere" (Alahmad et al. 2018, p. 1).

High availability environments rely on a number of feats of engineering, which are out of the scope of this paper, however some of the more important ones include avoiding single points of failure, having good redundancy among systems, and above all having robust and reliable technology. In terms of DDoS deterrence, availability requirements and the technological aspects associated with meeting these requirements cannot be overstated, as they lower attack impact and enable a speedy recovery, therefore warranting a more in-depth exploration in the following section.

2.2.1 Confidentiality, Integrity and Availability

Traditional IT information security is defined as the "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (FISMA 2014, 44 USC §3552; SANS Institute 2020). A 'denial-of-service attack' (DoS) is defined as "the prevention of authorized access to resources or delaying of time-critical operations" (Nieles et al. 2017, p. 78). The term 'denial-of-service' is autological, as such an attack attempts to deny legitimate users access to a particular online resource or service. It therefore primarily constitutes a threat to data availability, as well as to the infrastructural integrity of services on the Internet, as during a DDoS attack legitimate users will be "crowded out" from using a service and accessing data (Wang et al. 2017, p. 1).

In light of this, availability requirements and service guarantees form the basis on which the success rate of such attacks can be diminished, and their effects mitigated. Availability implies the continued functioning of all components that constitute the system, leaving room for numerous vectors of potential compromise. For example, disruptions to the smooth and synchronous functioning of hardware and software, as well as lack or exhaustion of critical system resources, such as network bandwidth, CPU power or electricity, can quickly result in "down time" (for a more elaborate list see Tchernykh et al. 2016, p.2). In order to mitigate the many aspects which can cause availability degradation, programmers and computer engineers developed the concept of utility computing, which aimed to make computing power available "on demand", whenever it is needed by a user – a point of reference which eventually also drove the development of the Cloud (Dean 2015, p.2). Cloud computing is therefore defined as,

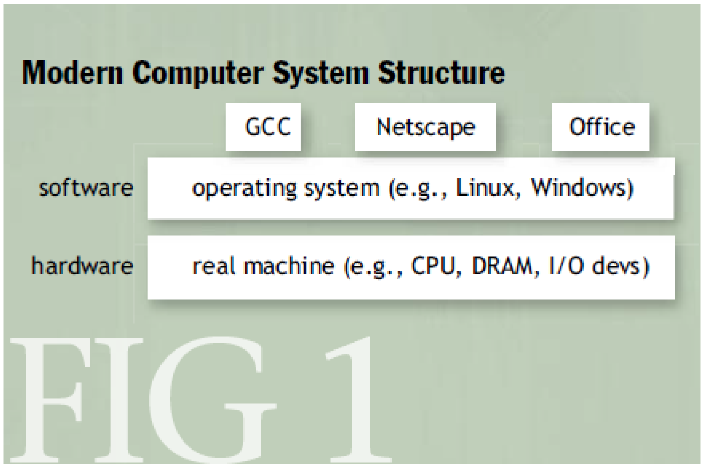
> "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Hussain et al. 2017, p.57).

Due to the increasing accessibility and affordability of PCs, utility computing at its onset took shape in a distributed and decentralized manner, as each user procured their own computer as a means of attaining their desired computational utility (Dean 2015, p.5). As the scale and diversity of computer systems grew, programmers and developers continued to struggle to attain a good balance between high performance computing, and fault tolerance (Dean 2015, p.7). The growth of datasets and resource-intensive interactive services to query and interact with all these datasets, such as search engines, required novel approaches to creating large-scale computational systems to match the performance requirements for these new structures (Dean 2015, p. 9). As Jeff Dean points out, "Basically the Web grew from millions to hundreds of billions of pages and you needed to be able to index it all, and then search it really fast. And be it, by requiring that you search it really fast you actually need parallelism across a very large number of computers” (Dean 2015, p.9).

2.2.2 Virtualization

The need for greater parallelism across a wide range of machines combined with the heterogeneous and extensive failures that regularly result in such computer clusters led to the realization that the reliability requirements demanded by modern high availability computer systems must ultimately be guaranteed by software (Dean 2015, p.15). In order to guarantee the reliability and scalability of large clusters, the software had to enable the systems a measure of self-management and self-repair, which was achieved by abstracting away or ‘virtualizing’ resources that could be shared across the cluster and therefore managed from a control node (Dean 2015, p.16). For a more elaborate description of this concept see Rosenblum 2004.

Rosenblum 2004, p.36


Modern Computer System Structure
GCC
Netscape
Office
software
operating system (e.g., Linux, Windows)
hardware
real machine (e.g., CPU, DRAM, I/O devs)
FIG 1

The advent of virtualization has changed the notion of data centres from being warehouses of cumbersome and inflexible physical servers such as mainframe computers, to having abstracted physical hardware to create “large aggregated pools of logical resources” that are offered to customers in the form of virtual machines (Oracle Corporation). This consolidation allows for greater and more efficient sharing of tangible, limited and expensive resources, including everything from CPUs, storage, applications and applets, containerization software, memory, network bandwidth, and others (Oracle Corporation). Due to the intervention of virtualization software within the system layers, the Virtual Machine Monitor or Hypervisor, can control a large number of virtual machines from a single point, greatly easing the management of computer clusters, but also creating redundancy to the extent that hardware failures no longer result in unavailability of services, but rather only reduce the pool of available resources (Rosenblum 2004, p.40).

While virtualization does not prevent DoS and DDoS attacks from directly targeting systems (virtual or physical) by exploiting weaknesses or vulnerabilities that render said systems unavailable, the advent of virtual, cloud-based computing implied that resource exhaustion attacks would necessarily have to exhaust ever greater pools of clustered resources. At the same time however, disruptions of these clusters would affect greater numbers of users who rely on these aggregate resources.

2.3 Evolution of (D)DoS

Since early DoS attacks were usually focused on flooding the network and transport layers (OSI Layer-3 and Layer-4), they were mostly accomplished by exploiting vulnerabilities on network protocols or devices including hubs, switches, bridges, modems, gateways, routers and firewalls, in an attempt to disrupt the forwarding procedures on these devices to incapacitate traffic flow to and from a network (Wang et al. 2017, p.1). While many attack vectors can lead to unavailability, DoS attacks do not necessarily have to be complex engineering endeavours, but can be, as the definition suggests, any action that renders a device unavailable to a legitimate user. As IT security and particularly security of network devices matured, making them unavailable was in most cases no longer as simple as running a single, remote command (see example of David Dennis - Verma et al. 2018, p. 108; Radware 2017). Malicious actors had to increasingly look for vulnerabilities that could be used in combination with one another to exploit weaknesses leading a device to crash, or otherwise compromising its availability. Such vulnerabilities are not limited to only the device's software (think code errors, buffer overflows, etc.) and hardware (resource limitations), but also extend to vulnerabilities on a protocol level and weaknesses in the inherent design and engineering of the Internet, which will be explored in later chapters (Wang et al. 2017, p.2; Feng 2003, p.322; Hoque et al. 2015, p. 2242; Mirkovic and Reiher 2004, p. 40).

2.3.1 The Morris Worm

An interesting example illustrating the above concept of multi-vector systems compromise was the Morris Worm of 1988 that during the course of its operation indirectly caused one of the first major distributed denial-of-service (DDoS) attacks on the then ARPANET infrastructure, the precursor to the modern Internet. A computer worm is self-replicating code of which the primary aim is to propagate to as many hosts as possible, as efficiently as possible, to subsequently execute complex routines on the target system (Cole 2009, p.199). Besides replicating and propagating, worm code can also be damaging or destructive to systems as it often alters, harvests or destroys data (Cole 2009, p.200). The general characteristic of computer worms of mounting active instead of passive attack patterns means that the worm is constantly searching for new hosts to attack, with a distinct list of priorities and operations that it needs to execute to either infect hosts or mark them as "immune" or "infection-proof" (Seeley 1989, p.7).

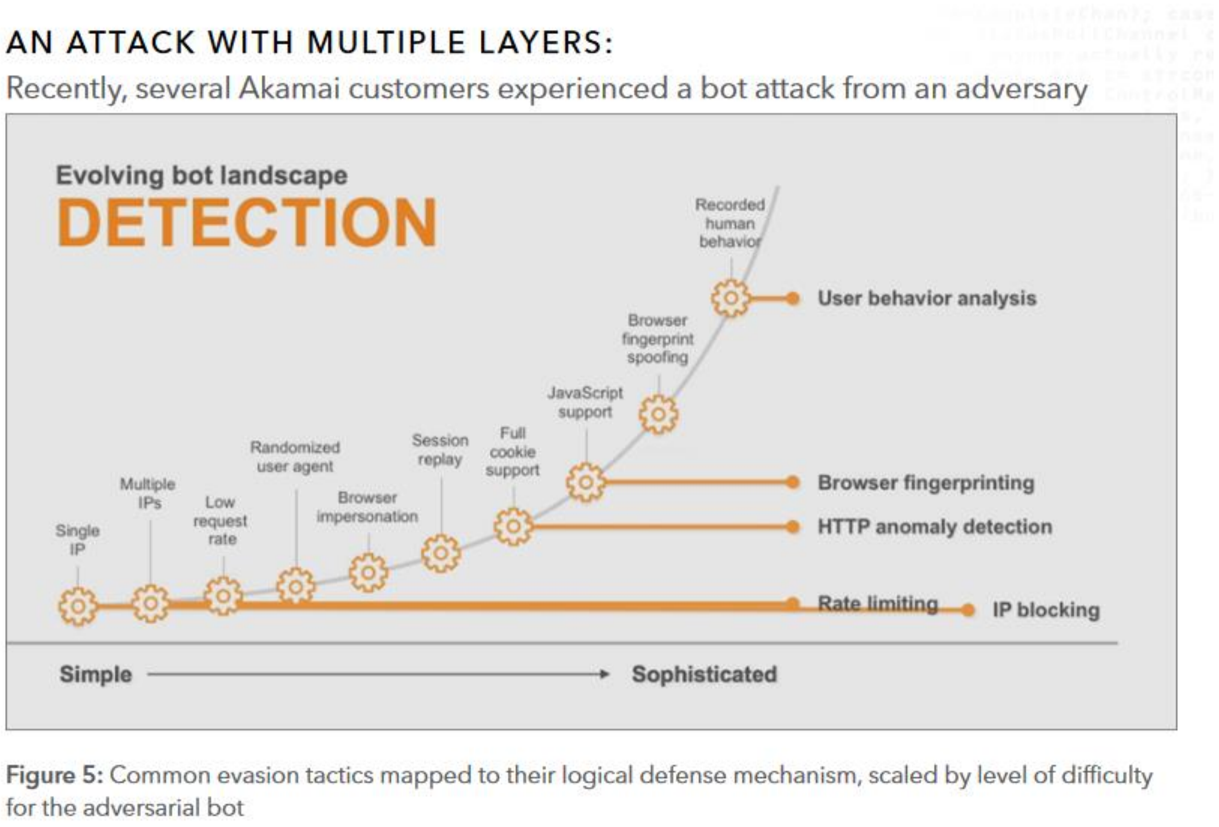
It is generally regarded that the Morris Worm was not written to purposefully damage ARPANET machines that it targeted, however the exploit code was written to compromise a number of programs running on top of the TCP/IP stack including *rsh, rexec, fingerd,* and *sendmail,* using multiple methods including buffer overflows and brute force (Seeley 1989, p. 8-9). In order to maximize the chances of infection, the worm code was written to try running specific routines designed to exploit weakness in the aforementioned programs in an orderly fashion. If one routine failed, the code would invoke a different routine to try to gain access and infect a host. While the worm had a method for listing hosts it propagated to as "infected" or "immune" in order to avoid running on the same host multiple times, however these controls ultimately proved ineffective at keeping this from happening (Spafford 1988, p. 14; Seeley 1989. P.9). This effectively resulted in multiple worms running concurrently on the same system, thus increasing the load and straining system resources, including to the point of system crash (Spafford 1988, p.11).

While the Morris Worm was not designed to steal information, harvest passwords, or cause damage to computers and networks, the design of the code that constituted it consumed CPU time, network bandwidth, and other resources, eventually overwhelming ordinary user processes and requests and leading them to fail on multiple endpoints, thus resulting in a broad DDoS across the entirety of the network (Seeley 1989, p. 13). As the worm prioritized infecting network gateways, to subsequently be able to reach more potential victim hosts, the effects on the ARPANET were severe, with network administrators having to shutdown gateways and other infrastructure in order to isolate and destroy the worm (Seeley 1989, p.13). This both advertently and inadvertently rendered significant amounts of the network and the services running on it unavailable for legitimate users, including the exchange of electronic mail, through which purportedly also the instructions for mitigating the worm infection were issued but received with days delay as a result of the on-going attack (Seeley 1989, p.13). Estimates put the number of infected machines at 6,000 in the first few hours of the worm’s deployment alone, which is especially telling given the fact that the ARPANET constituted a total of approximately 60,000 nodes at the time (Denning 1989, p.530).

The Morris worm demonstrated a number of novelties with regards to DoS attacks, and also indicated the path of development of DDoS attacks that would appear subsequently. Firstly, the worm demonstrated that a DoS attack, far from only flooding a target, can manifest as a result of complex and interdependent attack patterns, involving multiple phases and multiple vectors of compromise including the use of worms. Secondly, it demonstrated that if measuring attack effectiveness as the extent to which network operations are disrupted, a network of attacking nodes is more effective in creating a DoS scenario than a single source node. Thirdly, worm code often embeds itself in binary executable files to execute complex routines, making it difficult to purge once it has infected a system (Cole 2009, p.200). This implies that the distributed attacking systems (DDoS sources) will be more resilient towards defensive efforts on the part of network and systems administrators, resulting in prolonged DDoS attacks due to the more extensive mitigation efforts that will be required to purge the malware from infected systems and stop the attack. Finally, the worm illustrated that (D)DoS attacks are not a unitary concept that can be mitigated with a few lines of code but that such attacks can also be complex, involve a combination of multiple concurrent attack patterns and can materialize as a result of compromises of critical aspects of the Internet’s design and functionality.

2.3.2 Botnets and the Emergence of DDoS

The novelties demonstrated by the Morris worm were not taken for granted by would be DoS attackers who quickly used these techniques to develop what became known as Distributed Denial-of-Service (DDoS) attacks. These cybercrime entrepreneurs began utilizing worms to infect and “recruit” networked devices into Botnets that were capable of launching DoS attacks from multiple, coordinated and distributed source nodes. A Botnet is a network of computers – often called 'zombies' – that are centrally controlled by an operator – sometimes called a 'Botmaster' – who implements various Command & Control (C&C) strategies to control their behaviour (Hoque et al. 2015, p.2243; Alomari et al. 2012, p.25). Bots are essentially scripts running on a victimized device with the aim of performing automated functions on behalf of the operator (Alomari et al. 2012, p. 24). A full taxonomy of bots and their uses is out of the scope of this research paper however, it is relevant to illustrate their role in enabling DDoS attacks.



AN ATTACK WITH MULTIPLE LAYERS:

Recently, several Akamai customers experienced a bot attack from an adversary

Figure 5: Common evasion tactics mapped to their logical defense mechanism, scaled by level of difficulty for the adversarial bot

(McKeay et al. 2019b, p.18)

Hoque et al. (2015) outline a number of benefits associated with using botnets for DDoS, including:

- The large number of compromised nodes allows for quick and powerful flooding attacks;
- Identifying the attacker becomes difficult due to the distributed nature of the attack and the fact that it is using otherwise legitimate hosts;
- Botnets generate both legitimate and illegitimate traffic, making it difficult to distinguish between the two and identifying the attack in real time.

Setting up and effectively using botnets is however no easy task and forms an operational precursor to the would-be DDoS attacker. There are generally three phases described in the botnet formation process including *recruitment*, *exploitation* and *infection* (Mirkovic and Reiher 2004, p. 40). Incorporating this topology with that of the DDoS attack itself as shown below, these three aspects operationally take place during phases (i) and (ii) of the DDoS attack, as outlined by Hoque et al. (2015):

Phase:	**Explanation:**
(i) Information gathering / Recruitment	Mostly marked by an automated effort to scan the Internet for potential vulnerable hosts, the information gathering and recruitment phase focuses on gaining the necessary information to create an attack scenario by identifying weaknesses on Internet connected hosts to later infect them and use them as bots. Any information pertinent to the specific target would also fall in this phase.
(ii) Compromise / Infection and Exploitation	The hosts identified in phase (i) are infected with malware or exploited by a different means to attach them to the Command and Control infrastructure built by the attacker.
(iii) Attack	The various, distributed, compromised hosts are used to flood or otherwise deny a service on a target system.
(iv) Clean-up	Any evidences such as log files or records are purged from memory and disk of the compromised hosts.

(Hoque et al. 2015, p.2242; Mirkovic and Reiher 2004, p.40-41)

Due to the complexity of this kind of cybercrime, comprehensive deterrence would require some kind of deterrent intervention in multiple infrastructural and geographical locations, such as the source and destination networks, but also by multiple populations, from the average laptop or IoT device owning end-user, to the administrators of highly dynamic, enterprise environments. Due to the difficulties and limitations of conducting in-depth measurements in all these different environments and scenarios, a comprehensive mapping of DDoS deterrents throughout the local and public networks is difficult and also out of scope of this research paper, which given its scope, breadth and data availability limitations instead focuses specifically on the DDoS attack phase itself. Due to an inability of most system administrators to intervene in public, non-trusted networks, deterrence by denial strategies focusing on defence and resilience become an important paradigm by enabling potential victims to fend off what are often seen as inevitable attacks. In order to determine the most effective way to change the cybercriminal's decision calculus to deter DDoS attacks against virtualized environments, the theoretical limitations for criminological deterrence must first be understood, which will be explored in the following sections.

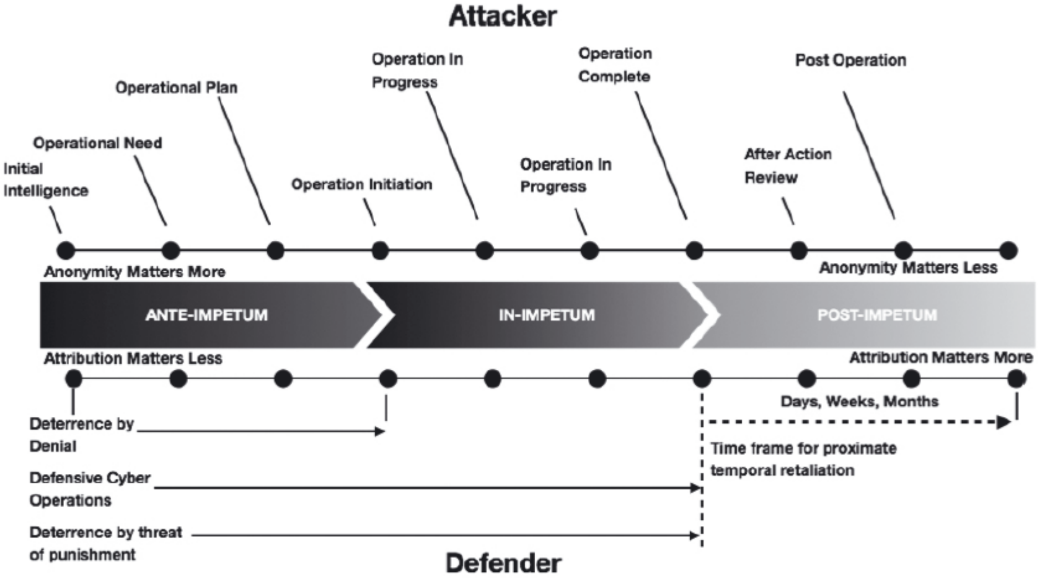
2.4 Limitations of Cyberspace Deterrence:

The above characterisation of cyberspace implies that any effective deterrence approach must take account of the complexity and sheer breadth of the various layers, aspects, and features of this domain, as well as its interaction with the physical world, if it is to be effective. The topography of deterrence must thus overcome the traditional dichotomous conceptualization consisting of clearly defined cause and effect analyses and game theoretic calculations, and be extended to subsume the complexity of the new, virtual conflict spaces. In this regard, Alex Wilner argues that the recent transposition of deterrence theory into the cyber realm “skewed the nascent literature on cyber deterrence in particular ways” (2020, p.256).

Namely, Wilner states that the firm theoretical focus on deterrence by punishment in traditional deterrence literature (see Akers 1990, p.660) has led to a neglect of other relevant deterrence concepts, including denial, dissuasion, influence and delegitimization (Wilner 2020, p.256). Deterrence fundamentally relies on convincing an adversary to refrain from committing an unwanted act, therefore “at its theoretical core, [it] entails using threats to manipulate an adversary’s behaviour” (Wilner 2020, p. 248). In that regard, deterrence techniques can be broadly classified into two general categories of ‘active’ and ‘passive’ deterrents (Trujillo 2014, p.45). Deterrence by punishment is commonly classified as ‘active’ deterrence, while deterrence by denial is classified as ‘passive’, also known as ‘latent’, deterrence (Trujillo 2014, p.45). The broad distinction between the two lies in how the deterrence effect is achieved. While active deterrence consists of threats of punitive measures, such as counter-hacking, physical imprisonment, (a)symmetric retaliation and other reprisals, passive deterrence does not direct counteraction against an attacker but rather consists of preventive, defensive and resilience strengthening measures that will dissuade an attacker or nullify potential gains (Trujillo 2014, p.45). Both approaches attempt to target and operate against the decision making calculus of potential attackers by targeting four key factors, including:

1. Gain value (i.e. the benefits of an attack to the attacker);
2. Gain probability (i.e. the probability of the attacker achieving those benefits);
3. Loss value (i.e. the costs the defender will impose on the attacker);
4. Loss probability (i.e. the costs the attacker foresees being imposed).

(Cooper 2012, p.109; Brantly 2018, p.37).



(Brantly 2018, p.46)

While threat of punishment can be a valid tool for deterrence in cyberspace, it is a dubious one at best, as it presents a number of implementation problems for the victim (see Brantly 2018, p.46; Trujillo 2014, p.45; Cooper 2012, p.109). In most judicial systems around the world, the burden of proof lies with the authorities who are required to identify the perpetrator and prove that an illegal act was committed (Brantly 2018, p. 45). A prerequisite of punishment is therefore knowing who the perpetrator is, and due to the technical design of the Internet, attribution of action to a particular user, and by extension to a particular individual, is difficult and time consuming at best (Brantly 2018, p.46; Cooper 2012, p.106). The "who, what and why" in cyberspace can be frustratingly difficult questions to answer, meaning that the preconditions of certainty and celerity are not guaranteed. Proportionality of response with regards to non-physical punishment (i.e. online market takedowns, shutting off servers, counter-hacking, blacklisting, etc.) is also difficult, brings asymmetric outcomes, and is likely to take some time. These factors combined would suggest that the traditional criminological deterrence formula of certainty, severity and celerity is not relevant in the digital era.

In addition to the deterrence problem, deterrence by punishment in cyberspace is also limited by its ability to signal and guarantee the credibility of retaliatory threats. Signalling in cyberspace is ambiguous to say the least (Brantly 2018, p.44). From the get-go, the attribution problem limits any ability to directly communicate and therefore signal or convey credibility to potential attackers. The tight binding between punishment and the problems of attribution, signalling and credibility demands a reinvigorated focus on alternative concepts of deterrence that "form the basis for most deterrent and compellent engagements" (Winler 2020, p.248; Cooper 2012, p.106). Apart from punishment these can include also denial – generally consisting of depriving an opponent of expected benefits of a malicious act – and delegitimization, dissuasion and influence (Wilner 2020, p.248). Due to the boundaries and limitations of this thesis project, dissuasion, influence and delegitimization are out of scope of this research paper. As previously mentioned, deterrence by denial is further made up of two components consisting of resistance and resilience.

2.5 Internet Design and DDoS Contributing Factors

The immense and unexpectedly efficient damage wrought by the Morris worm sparked various discussions on the design of the ARPANET, and subsequently the Internet, and its vulnerability to network-based attacks (Feng 2003, p.322). Ironically, Wu-Chang Feng points out that if anything, the Morris worm actually definitively proved the effectiveness and strength of the Internet's design, as the speed with which it was able to spread from host to host attested to the efficiency of the interconnectivity and data travel between the nodes on the network (Feng 2003, p.322).

The nature and engineering design of the contemporary Internet infrastructure relies on a number of factors that either directly or indirectly enable DDoS attacks to take place. The primary role and design of a network is usually to "make efficient use of shared assets among network users", focusing on the effectiveness of packet transmission from the source to the destination (Hoque et al. 2015, p. 2242; Mirkovic and Reiher 2004, p. 40). This notion is known as the *end-to-end paradigm*, where the "intermediate network provides the bare minimum, best-effort packet forwarding service, leaving to the sender and the receiver the deployment of advanced protocols to achieve desired service guarantees" (Mirkovic and Reiher 2004, p.40). In the end-to-end design, particularly the protocols running on the network and transport layers (Layer-3 and Layer-4 of the OSI model) are marked by their simplicity and broad compatibility, pushing out the complexity to the higher layers while leaving the underlying network simple, efficient and fast (Feng 2003, p.323). Due to the Internet's design also primarily aiming to provide a free medium of information exchange, there is usually minimal intervention in the intermediate network between two communicating hosts, guaranteeing that the public network is optimized for packet forwarding, not to stop any illegitimate or malicious traffic (Mirkovic and Reiher 2004, p.40). Mirkovic and Reiher (2004) identify five aspects of the Internet's design that broadly enable the technical feat of launching a DDoS attack, including that:

1. Internet security is highly interdependent;
2. Internet resources are limited;
3. Intelligence and resources are not collocated;
4. Accountability is not enforced;
5. Control is distributed.

These five aspects will be explored more in-depth in the following sections.

2.5.1 Internet Security is Highly Interdependent:

As was outlined earlier, intermittent nodes that communicate via the Internet are often subverted through security compromises for subsequent use as launch points for DDoS attacks (Mirkovic and Reiher 2004, p. 40). For this reason, the security state of these nodes and the rest of the Internet infrastructure directly affects the susceptibility of other systems to DDoS attacks (2004, p.40). Botnet formation and maintenance is an effort intensive exercise, which is made significantly easier through selective targeting of networked nodes that are poorly secured and therefore more easily subverted. The greater the numbers of such nodes that are attached to the botnet, the stronger the potential potency of the attack and therefore also the higher the benefit for the attacker. As these nodes are often external to the network of the target, there is a considerable amount of security interdependence due to the fact that the defender inadvertently relies on the security of these intermittent, networked parties if it wants to avoid victimization (Houle et al. 2001, p. 2; Miura-Ko et al. 2008, p. 68; Mirkovic and Reiher 2004, 40). Because of this, the lack of information security in the wider parts of the public network "is often considered to be a negative externality much like air pollution" (Miura-Ko et al. 2008, p. 68).

"The establishment of credible deterrence by denial thus often starts with the allocation of financial capital to purchase technical resources and provide human capital sufficient to continually update, enhance, audit and manage complex network infrastructure" (Brantly 2018, p.47). Network participants can create positive externalities by investing in information security and good “digital hygiene” by regularly patching and maintaining updated systems, and thus ultimately help in reducing the potency, damage and likely also the frequency of occurrence of DDoS attacks (Miura-Ko et al. 2008, p. 68). Such investments can be directed broadly into various administrative, technical and physical controls that enhance information security and could range from network-based to host-based defenses, including but not limited to anti-virus products, firewalls, intrusion detection/prevention systems, and others, which will collectively increase the difficultly of adversaries to intrude into a given network and assemble botnets (Brantly 2018, p.47). In addition, administrative controls such as security awareness training are critical in stimulating end users and administrators alike to be more conscious and diligent when it comes to securing their devices. Secure network architecture design and diligent security administration on the part of network participants implies that additional costs are being imposed on the attacker and better resource allocation is being done by the defender, and thus demonstrating to potential adversaries that the probability of success is low (Brantly 2018, p. 47). Virtualized environments in addition offer better economies of scale for information security expenditures, as the same solutions can be used to defend a multitude of servers, while an individual PC owner would have to invest time, money and effort for themselves to create all like defences individually either on their local network, or on each individual PC.

However similar to the defender, the attacker is also forced to make expenditures and certain weigh-offs with regards to the effort and time he/she is willing to invest in particular phases of the DDoS attack. For example, different scanning and exploitation strategies will yield different results with regards to the variety of machines detected to be online and the vulnerabilities present that will exploit the availability of these machines (Mirkovic and Reiher 2004, p.40). As such, the attacker will most likely follow the path of least resistance to achieve their overall aim. Layered defences and strategies such as defence-in-depth (DiD) will therefore create obstacles in this path during all of the phases, lowering the probability of success, and increasing the loss value and probability for the attacker, therefore potentially deterring the attacker by forcing him to abort the operation at multiple, consecutive stages of the attack. While DiD is quite a broad concept, roughly implying that a defender implements plural and redundant security controls in preparation for the eventuality that one or more of them should fail, its implication can be taken some steps further and more specifically defined (Pfleeger et al. 2015, p.30). A pre-condition of DiD is that the defender implement full spectrum defence by focusing on controls within the domains of people, processes and technology (Cole 2009, p.38). Further from this however, and specifically in terms of network security, DiD implies that control redundancy is particularly persistent in terms of boundary defence, network layer segregation or critical data isolation, and encryption (Cole 2009, p.38). In order to meet this requirement, controls must be required at least in the people, processes and technology domains, and require at least two of the above defence principles. In terms of controls, these could include but are not limited to deploying information protection mechanisms in multiple places throughout the network, maintaining secure network boundaries through the use of firewalling, maintaining detection mechanisms and sensors (e.g. IDS/IPS) at each boundary and protecting data with tokenization or other form of data protection (Cole 2009, p.40-41).

2.5.2 Internet Resources Are Limited:

As already discussed in depth in previous sections, many (D)DoS attacks are resource exhaustion attacks which aim to "use-up" all the available resources in order to "crowd out" the legitimate users and their requests. This is possible due to the fact that the infrastructure and systems that comprise the networks that communicate via the Internet are composed of limited resources that are required for continued system functioning (Houle et al. 2001, p.1). These include but are not limited to electricity, CPU, memory, storage, etc. Guaranteeing and securing the continued availability of these resources implies that successful (D)DoS attack scenarios will be harder to achieve, hence lowering the gain probability for the attacker, and have fewer direct- and side-effects, thus lowering the gain value as well. Virtualized environments, and the aggregated pools of distributed resources that they compose, offer better load balancing and resource optimization through easier, more efficient and more effective allocation of resources to the system where they are required. Virtualization created a revolution in elasticity of demand due to the ability to easily spin up new VMs and allocate new resources on-demand when these are required, a function also known as "auto-scaling" (Somani et al. 2017, p.31). Traffic is automatically rerouted to underloaded nodes to avoid overload on parts of the infrastructure, responding to workload requirements in real time, and scaling down when processing returns to normal (Tchernykh 2016, p.5). This workload elasticity will ensure that the Quality of Service (QoS) is guaranteed also during peak runtimes or in adverse circumstances such as during a DDoS attack, but also that the systems are idle during troughs therefore avoiding unnecessary resource consumption when these are not needed (Tchernykh 2016, p.5).

Similarly, in terms of availability if a VM becomes unavailable the virtual backup image or container can be spun up on a different hypervisor and restore the exact same system within minutes. "In virtualized architectures and especially in the cloud, it is common to move VMs from one VMM to another at runtime; this is called VM migration, for example, for balancing the load between hardware nodes" (Jahanbanifar et al. 2014, p.40). As a result, the hardware nodes represent a potential single point of failure, a risk that must be mitigated by ensuring that there are other redundant nodes capable of carrying the load in cases of failure on the primary node (Jahanbanifar et al. 2014, p.40). Redundancy is a requirement that can be applied very broadly as well as very granularly, as for example many organizations will maintain a redundant data centre in passive mode to which they can revert to in cases of unavailability of the primary data centre. However, on a smaller scale, spare parts for highly available machines are a must in case any or some of the hardware components fail and require replacement. Data minimization furthermore assists with minimizing the load on the network infrastructure, leaving more resources available to withstand network attacks. Even more significantly, following the data minimization principle ensures that enterprises retain only the data that is necessary for functional purposes, therefore reducing the number of records that will be lost or leaked in the event of a successful attack.

2.5.3 Intelligence and Resources Are Not Collocated:

The philosophy of the end-to-end paradigm implies that the network and transport layers (OSI Layers 3 and 4) are composed of lightweight and broadly compatible protocols that are capable of utilizing speed and simplicity to limit the amount of processing required to route traffic as quickly and cost-efficiently as possible between two endpoints (Mirkovic and Reiher 2004, p. 40). As a result, and due to the desire for high throughput on the Internet backbone, the intermediate network is usually composed of high bandwidth pathways, while end networks usually reserve only as much bandwidth as they require due to cost and other considerations (Mirkovic and Reiher 2004, p. 40; Doerr et al. 2012, p.45). This means that in the case of DDoS attacks, the routes that forward the payload packets through the Internet and to the target allow for much greater throughput and as a result deliver many more requests than can be processed at the target endpoint, quickly leading to bandwidth exhaustion.

Wider and more extensive network infrastructures partially ameliorate this problem simply due to their relative size and higher bandwidth capacity. Nonetheless, the underlying issue remains, no matter what the scale of the network. ENISA, the European Networks and Information Security Agency, recommends a combination of redundancy and resilience measures on the structural, network-design level to help mitigate this problem. The aim being for the operator to maintain an acceptable level of network operation also during times of high impacting crises (e.g. DDoS attacks, earthquakes, large-scale failures), ENISA recommends following the principle of resource duplication (Doerr et al. 2012, p.34). This implies that the operator will over-provision resources throughout the system by maintaining multiple independently operating units that are individually capable of handling peak demand that can arise in times of high stress on the network (Doerr et al. 2012, p.34). A common baseline for over-provisioning is a factor of 2, implying that all primary equipment will be utilizing only 50% of its overall available capacity (Doerr et al. 2012, p.34). While applying this practice to all network components could result in immense additional cost for organizations, especially those with large enterprise networks, its selective use for critical components, pathways and applications would either lower the gain value or increase the loss value for the attacker. Namely, the over-provisioning would imply either that the attacker's output capacity would not be enough to achieve a denial of service, therefore erasing any gain, or that the attacker would have to invest in significantly more resources to succeed, thus increasing the costs incurred.

Some other strategies do exist for solving this problem, short of changing the entire philosophy of the Internet itself. Null, or “Black hole” routing is one such example, however since null routing does not discriminate between packets, but merely routes every packet destined for a particular IP destination to a null interface, the target will effectively still be under DoS (Stamatelatos 2006, p. 3). The purpose of this measure is therefore to avoid having collateral damage in other parts of the network, more so than countering the attack itself. Edge computing might be another such effort, which could end up transposing significantly more intelligence, usually belonging to the higher-level protocols, towards the network edge, however this concept is still largely theoretical and is intended solely for Quality of Service and not security guarantees (for more detail see Ahmed et al. 2017).

2.5.4 Accountability is Not Enforced:

The open nature of the Internet implied that security solutions that were implemented to enforce confidentiality, integrity and availability of the information transmitted over this infrastructure would necessarily have to take into account the inevitability of snooping and cross-reading of information without authorization. Without the intervention of dedicated security controls, the hosts on the same broadcast domain can listen to each other's transmissions, meaning that information broadcasted can be received by multiple hosts, even if this was not the intention. In light of this, security solutions such as encryption were developed, not to change the underlying nature of the information transmission, but to make information unintelligible to all but the intended recipient. An unintended side effect of this approach, however was that due to the anonymity of information and participants on the Web, accountability became much more difficult to enforce. Accountability is defined as "an obligation to accept responsibility for one's actions", but fundamentally relies on the identification of the sources of those actions (Mirkovic and Reiher 2008, p.45). IP spoofing, network address translation (NAT), DHCP and other innate characteristics of the IP/TCP protocol stack imply that IP addresses are not very reliable source identifiers of traffic and data being exchanged on the Internet (Mirkovic and Reiher 2008, p.45). The nature of the technology and the protocols which construe it implies that reliable identification and attribution of action using technical means is resource and time consuming, and as a result out of reach for the majority of the actors within the Internet space.

Yet, Mirkovic and Reiher's proposal for a capability-based mechanism to enforce accountability is largely grounded in the notion that accountability on the Internet should be possible by and large to subsequently punish any actors that are identified to have acted maliciously (Mirkovic and Reiher 2008, p.45). While this would be a viable step towards deterring by punishment, this paradigm is out of scope of this research paper. In light of this, accountability mechanisms within the paradigm of deterrence by denial are considerably different. Namely, the nature of today's Internet services are such that ever larger quantities of data are being collected, processed and shared among multiple entities, such as CSPs, to provide services to users who, more often than not, expect seamless user experiences (Pearson et al. 2012, p.629). This not only provides difficulties in terms of accountability, transparency and legitimacy for such processing, but due to the complexity of modern computing systems, also presents significant difficulties in terms of mapping and providing explanation to lay persons as to how, why and to what extent their data is being used, and what are the resultant risks (Pearson et al. 2012, p.629; Urquhart et al. 2019, p.4). The opaqueness in terms of who, where and why is holding any individual's data implies that users often remain unaware of the potential repercussions that could result in compromises or unavailability of their data, as in the event of a DDoS attack (Pearson et al. 2012, p.629; Urquhart et al. 2019, p.4). *En masse* data collection also implies that DDoS attacks will potentially render larger amounts of data unavailable and by extension impact a larger number of users.

In light of this, data processing risk assessments, data portability and transfer requirements, consent for processing, and organizational security responsibility definitions are key organizational and functional requirements for the control of risks and potential damage to users, that give the latter enhanced control over their own data as a result (Pearson et al. 2012; Urquhart et al. 2019). While these controls will not affect the potential DDoS attacker directly, their implementation will show effect in other ways. Namely, more awareness, accountability and sensibility towards critical data will imply that such data will be kept in fewer and more controlled systems, therefore targeting the attacker's gain value and lowering the risks of compromise and unavailability of such data as a result of collateral DDoS damage.

2.5.5 Control is Distributed:

As the Internet is construed by many individual networks, its management as a whole is distributed in nature (Mirkovic and Reiher 2004, p. 40). The owners and administrators of these individual networks all follow their own policies, procedures, technical designs and standards, making the universal deployment and harmonization of security controls and standards difficult to say the least (Mirkovic and Reiher 2004, p.40). As a means of strengthening resistance and resilience, legislation should thus aim to implement standardized baselines, policies, procedures and practices to as many entities and users as possible in order to ensure the implementation of equal standards in at least the basic security and control categories. These categories should ideally cover people, processes and technology, as outlined by the DiD framework (Lopes et al. 2019, p.3-4; Cole 2009, p.39). This would in turn target the attackers gain probability, loss value, as well as loss probability due to the better implementation of basic security and privacy standards across the Internet landscape, as well as the uniform implementation of these standards across all applicable entities. Due to the need for standardization across as many actors as possible, third party requirements are also worthy of examination, as these would extend the applicability of the controls also to third parties.

Security incident reporting on a wide range of information security issues, including breaches of all three categories of C-I-A, also presents a significant contributor towards better security on the Internet as a whole. As discussed in previous sections, information security incidents are in today's connected age increasingly becoming a fact of daily life. For this reason, incident response readiness is an important aspect of any information security management program. While not all incidents can be prevented, maintaining appropriate incident handling procedures enables organizations to respond quickly and effectively in an effort to minimize destruction and loss of data, mitigate weaknesses in the security framework and restore the availability of services (National Institute for Standards and Technology 2012, p.1). Furthermore, effective computer security incident response requires ancillary security capabilities that strengthen the overall security standing of a network. As an example, these could include monitoring systems, such as IDS/IPS and SIEM, that serve the purpose of incident and anomaly detection. Computer security incident management therefore serves the purpose of minimizing potential losses from DDoS attacks, therefore targeting and attacker's gain probability, and also indirectly increases the loss value for the attacker, as security incident management systems can potentially put pressure on the attacker in terms of attack resistance. Breach reporting also presents a significant contribution to better control and standardization across both public and private networks, systems and data spanning the Internet infrastructure.

In order to determine the study subjects' extent of utilization of deterrence by denial strategies, the aforementioned information security and data protection controls that mitigate these Internet design deficiencies, will function as positive indicators of resistance and resilience against DDoS attacks. To examine and test the research question, the following paper will apply a comparative case study approach comparing the presence and prevalence of these positive indicators within Dutch and American information security and data protection legislative frameworks.

3.0 RESEARCH METHODOLOGY

In order to examine the applicability of deterrence by denial theory on the mitigation of Internet design factors identified in the previous chapter, the research method will consist of a comparative analysis of key legislative documents that mandate the information security and data protection controls of cloud and virtualization technologies within the Netherlands and the US. To enable better generalizability, the focus of this research is not any particular legal or natural entity, or a particular cloud service or delivery model, rather it is the engineering of the Internet[5] itself that is uniformly applicable to all of its users. As such, the legislation that govern the many entities, both legal and natural, that utilize these environments, either directly or as a service, are many and wide due to ancillary regulatory requirements that are sector or service specific. Nevertheless, focus will be put on those documents that are considered key pieces of legislation within the general field and will be assessed for the resistance and resilience indicators that are mandated by them in an effort to answer the research question.

Research question:
To what extent are Dutch and American cloud services providers and other entities hosting virtualized computing environments obliged by legislation to implement resistance and resilience strategies that mitigate the DDoS enabling design aspects of the Internet?

3.1 Comparative Case Study Design

As the empirical phenomenon being studied is the inclusion of resistance and resilience strengthening indicators within information security and data protection legislation, the aim of this research design is not to directly deduce primary causal mechanisms of DDoS attacks. Rather, this descriptive comparative case study will aim to explore the extent to which the identified indicators are prescribed by the applicable legislation within the two countries, attempting to observe the differences in their respective deterrence frameworks. While a document analysis of legislative frameworks will not in itself offer enough empirical evidence to deduce primary causal mechanisms leading to particular DDoS prevalence rates in the two countries, the research will nonetheless test the value of deterrence by denial as a criminological theory in cyberspace. The method will observe whether the stark differences in outcomes between the two cases are aligned with legislative differences within a specific technological and criminological context through qualitative data analysis.

Towards this aim, a comparative case study design is preferred over other alternatives for a number of reasons. Firstly, DDoS being a criminological phenomenon, an experimental research design that would require any kind of manipulation of the relevant variables would be unfeasible within the scope and limitations of this research paper. A case study design allows for a narrowing of the scope through direct

[5] While an internet refers to a network of networks, the Internet as understood in this paper, refers to the global system of interconnected networks as defined by the Internet Engineering Taskforce (IETF) RFC1462 - https://tools.ietf.org/html/rfc1462.

observation of specific cases within the research framework in an effort to explain the differences in outcomes. The search for causality of criminal behaviour within the cyber domain is a daunting challenge. The low barriers of entry for potential attackers, numerous attack vectors and entry points, and the low costs of reiteration of failed attacks implies that such attacks will continue reoccurring due to a wide range of constantly changing causal mechanisms (Jabbour and Ratazzi 2012, p.37-39). As such, for the purposes of fulfilling the research goals of this paper, the intention is not to look for the causal mechanisms that lead to DDoS attacks as such, therefore working on the premise that such attacks are factually inevitable. It is rather to observe the technical permissiveness factors that subject systems to such attacks and to determine the extent to which these factors are obstructed through legislatively prescribed deterrence by denial controls in the two respective countries. Using a comparative case study approach to achieve this aim allows for the assessment of a wide range and variety of factors and evidences, something that would've otherwise been difficult in an experimental research design (Yin 2009, p.30). As such, deploying a case study design presents an opportunity to conduct an "empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin 2009, p.36). The holistic nature of the security and defence studies field, where multiple factors spanning multiple academic domains are observed to explain phenomena, implies that the phenomenon itself cannot be divorced from the wide range of contextual factors that construe it – context must therefore crucially be considered to avoid creating "controlled" and purely theoretical, empirical judgements that offer little value to real-world security challenges.

Secondly, as deterrence can hardly be claimed as the only influencing factor in the world of cybercrime, a specific comparative case study design doing an in-depth analysis of the deterrence by denial strategies of two cases is preferred over an approach that would assess multiple cases. The reason behind this is that a research design introducing multiple cases would be less capable of controlling a broad range of extraneous and otherwise influencing variables that might have an effect on cybercrime as a whole. By comparing two like cases with very different outcomes (high vs. low DDoS source attacks per capita), the existing design will most effectively reveal the theoretical mechanics that are under study in this paper and thus imbue more rigor than it would with an alternative design (Yin 2009, p.33).

Thirdly, the case study will not be generalizable to other countries due to the drastic differences in contextual factors, including Internet penetration rates, information security legislation, law enforcement and defence policy, but also in the frequency, strength and distribution of DDoS attacks across various nations and regions. However, this particular research design will instead enable analytical generalization of the technical and theoretical propositions established in this paper to all networks connected to the Internet (Yin 2009, p.33). While government policy and cybercriminal behaviour are subject to constant change and variation, the technical and theoretical propositions outlined in the study are generalizable to all Internet connected networks and DDoS scenarios. While technology also changes, the fundamental engineering of the Internet allowing for DDoS related cybercrime to take place, as outlined by Mirkovic and Reiher (2004), is in most cases the same everywhere in the world and subject to much less change and variation than policy or human behaviour.

3.2 Assessment Method

The primary method of this research paper will include document analysis of a handful of key pieces of legislation governing and regulating information security and data protection within the two case countries. Document analysis is defined as "a systematic procedure for reviewing or evaluating documents… in order to elicit meaning, gain understanding and develop empirical knowledge" (Bowen 2009, p.27). Document analysis is particularly applicable to qualitative case studies as it offers a wealth of data and descriptions of a single phenomenon, therefore assisting in developing a deeper understanding and insights of the problem area (Bowen 2009, p.29). Furthermore, government documents form an indispensable source of rich, high quality textual data that is generally considered to have high validity and trustworthiness due to its official provenance (Mackieson et al. 2018, p. 6). Due to the wide variety of possible computer architectures, cloud service and deployment models, as well as cybercrime deterrence methods, an analysis of legislation offers a way to generalize insights across a wide range of organizations, by controlling for contextual factors that might be sector or technology specific. To effectively assess and appraise the information that will be collected in these legislative documents, the content analysis research technique will be used.

While the primary method could be supplemented using method triangulation, which would be beneficial for corroborating the data acquired from the legislative documents, due to the scope, time and data availability limitations, this research paper will be a single-method case study (Bowen 2009 p. 28). The fact that legislative documents are publicly available information also assists the research in terms of feasibility, "facilitating expeditious identification of a complete data set, which is not always possible in qualitative research" (Mackieson et al. 2018, p.7).

3.3 Case Selection and Data Collection

When compared to the U.S. in the period between November 2017 and September 2019, the Netherlands was the source of 414,257,266 application attacks, consisting of primarily DDoS, while the U.S. was the source of 1,434,231,212 application attacks in the same period (McKeay et al. 2019a, p. 20-21). In per capita terms, the prior constituted as the source of approximately 24 attacks per citizen, while the latter approximately 5 attacks per citizen. While in aggregate terms the U.S. is clearly well ahead as mentioned previously, in per capita terms the numbers become strikingly dissimilar. Relative to its size, the Netherlands appears to have become a hub of DDoS related activity, becoming one of the primary sources of such attacks worldwide, even despite its relatively small size and as a result, relatively few internet users and Internet connected systems. This striking observation warrants a closer examination of the factors that are enabling such attacks in the Netherlands, especially given the changing technological context within which they are taking place. Furthermore, the two countries are relatively similar in nature, both constituting highly developed and digitalized, global economies, therefore setting a like-for-like environment in which the deterrence framework differences can be accurately identified. According to data collected by the World Bank, the Internet penetration rates in these two countries in 2018 were very similar, 93.29% in the Netherlands and 87.27% in the US, and both have had an approximately equivalent widespread exposure to the technology (World Bank 2021). The two countries are both pioneers in digital development in various societal, economic and political fields, both maintaining lead roles in e-commerce, digital identity technology (e.g. DigiD) and other Internet-based development. While the countries do not resemble in terms of population or geographical size, these factors are arguably less relevant in the context of digitization and online activity. Similarly, with respect to data centres and virtualized/cloud data processing, both countries are leaders in terms of sheer numbers and development of data centres and data processing facilities (Cloudscene 2021; Uptime Institute 2021). On an analysis level, the two countries also have comparable legislative regimes, which makes them good candidates for a comparative analysis. While the legal norms, codes, practices and the type of judicial environment are different, the two nevertheless have comparable federal/state level legislation for data protection and information security. While the US' standard practice is to create Federal as well as State laws, the Netherlands is also governed by EU laws and national legislation. Although these are not exactly the same legal mechanisms, they provide a comparable backdrop in which legislation of both countries can be assessed.

While there are many legislative and regulatory documents governing and regulating the processing, storage and transmission of information and data in terms of security and privacy, their applicability often varies depending on the type of industry and services being offered. Virtualized and cloud-based environments often pose regulatory difficulties to organizations, as these may no longer have full control over their operating environment, systems and data due to these components having been outsourced to a CSP (Cybersecurity and Infrastructure Security Agency 2018, p.100). While doing so provides these organizations with significant advantages, they will still be held to account for any non-compliance with applicable security and privacy standards and requirements enforced by the regulators (Cybersecurity and Infrastructure Security Agency 2018, p.100). As a result, legal and regulatory compliance is fast becoming one of the most important Non-Functional Requirements (NFR) for many organizations (Yimam and Fernandez 2016, p.1).

In order to support business and expand their services offering, many organizations must comply with multiple regulatory frameworks, spanning federal and state regulations, as well as industry and service specific regulations (Yimam and Fernandez 2016, p.5). In light of this, CSPs and equivalent providers often hold a wide array of certifications to ensure security coverage for multiple clients and in multiple areas, including for example business continuity (ISO 22301), information security management (ISO 27001), healthcare data protection (HIPAA, HDS), financial data protection (PCI-DSS, OSPAR), occupational health and safety assurance (ISO 45001), and standards for internal organizational controls (ISAE 3402, COBIT), to name a few. In an effort to increase generalizability and validity of the results, this research paper will focus only on tailored national level rules and regulations that uniformly apply to a wide variety of organizations and are not limited only to specific industries or services, or governed only on the basis of international standards. In this regard, the Cybersecurity and Infrastructure Security Agency (CISA) identifies the following as key pieces of legislation governing cloud services provisioning:

- Federal Information Security Management Act (FISMA);
- Healthcare Protection Portability and Accountability Act (HIPAA);

- Sarbanes-Oxley Act (SOX).

(Cybersecurity and Infrastructure Security Agency 2018, p.100).

In the Netherlands, the National Cyber Security Centre (*Nationaal Cyber Security Centrum* – NCSC*)* identifies the following as key pieces of legislation governing cloud services provisioning in the Netherlands:

- General Data Protection Regulation (GDPR) (*Wet Bescherming Persoonsgegevens*);
- Information Security for the National Services Decree (*Voorschrijft Informatiebeveiliging Rijksdienst – VIBR*);
- Information Security for the National Services Decree – Special Information (*Voorschrijft Informatiebeveiliging Rijksdienst – Bijzondere Informatie – VIBR-BI*);
- Archive Law (*Archiefwet – AV*);
- Security Investigations Act (*Wet veiligheidsonderzoeken – WVO*);
- Telecommunications Act (*Telecommunicatiewet – TW*);
- Computer Criminality Act (*Wet Computercriminaliteit – WC*);
- Government Information – Public Access Act (*Wet Openbaarheid van Bestuur – WOB*);
- Administrative Electronic Traffic Act (*Wet Elektronisch Bestuurlijk Verkeer – WEBV*).

(Nationaal Cyber Security Centrum 2012, p. 10)

Since the above date, the list has been supplemented by another crucial piece of legislation, the Directive on Security of Network and Information Systems (NIS), which will also be included in scope. As European directives are transposed into national legislation, the source document for the analysis will be the *Wet beveiliging netwerk- en informatiebeveiliging* (Wbni) that codified the NIS directive into Dutch national legislation. While FISMA and HIPAA explicitly mandate information security and privacy safeguards and requirements for their target audience, SOX does so only implicitly, with its primary focus being internal organizational controls aimed at strengthening the accuracy of financial reporting and accounting (Wallace et al. 2011, p.185-186). As a result, SOX compliance does not mention any specific IT security controls directly, which has resulted in companies seeking compliance with other standards, mainly ISO 17799, to achieve SOX compliance (Wallace et al. 2011, p.185-186). Likewise, the VIBR and VIBR-BI also merely refer the participants to comply with ISO 27001, as opposed to outlining any specific controls or requirements, therefore they will be excluded (Voorschrift IBR 2007). For the above reasons, these laws are not directly pertinent to the aims of this research paper and will be excluded. The *Av, Wvo, Tw, Wob,* and *Webv* are likewise only implicitly related to the information security and privacy of cloud services, and do not cover specific security controls, therefore they will likewise be excluded from the analysis for validity and feasibility reasons. While the Dutch Computer Criminality Act could be juxtaposed to the U.S. Computer Fraud and Abuse Act, these pieces of legislation are geared towards enabling criminal persecution of cybercriminals, therefore constituting deterrence by punishment and falling out of scope of this research paper.

While the GDPR is much more comprehensive in terms of applicability and coverage, regulating any professional or commercial entity (public or private) that processes any information that can potentially identify a natural person (i.e. Personally Identifiable Information – PII), HIPAA and FISMA are more limited in scope (Regulation 2016/679/EU, p. 3). In the case of the prior, it is applicable to only those organizations that process Protected Health Information (PHI), while the latter applies to all government agencies and affiliated organizations that use or operate any component of the national information system (FISMA 2014, 44 USC §3552; Yimam and Fernandez 2016, p. 4). The NIS Directive similarly applies to a specific scope of service providers, including CSPs, however is limited to providers considered vital for the national economy (Art. 3 Wbni, 2018; Ministerie van EZK 2018, p.3).

While CSPs often comply with multiple regulatory and legal frameworks, as previously mentioned, therefore likely having cross applicability between all of the above four key pieces of legislation, respective of the country, this assumption cannot be made for individual organizations that build and operate their own, on-premise, cloud-based virtual environments. This gap in the legislative framework is made worse by the more polycentric nature of the U.S. information security and data protection legislation, which is marked by a “multi-level, multi-purpose, multifunctional and multi-sectoral” character (Williams 2020, p. 232). In order to interpret these legislative documents in a comparable way, the fundamental differences in their regulatory models, regulatory applicability and jurisdictional differences will also be assessed.

3.5 Validity and Reliability

To ensure objectivity during the iterative process of skimming, examining and interpreting the data associated with the document analysis method, the analysis categories have been clearly and precisely defined to ensure replicability and reliability of the obtained results (Mackieson et al. 2018, p.4; Lopes et al. 2019, p.3). In order to increase the validity of the results, the scope of the analysis is also limited both theoretically to the framework of inherent weaknesses of the Internet allowing the phenomenon of (D)DoS attacks, as identified by Mirkovic and Reiher (2004), and contextually to only virtualization based cloud computing architectures. Therefore to enhance objectivity and avoid researcher bias, the content is “analysed in relation to all the meaningful categories” that are within the scope of this research paper, with clearly defined, documented and substantiated value assumptions made during argumentation (Lopes et al. 2019, p.3; Mackieson et al. 2018, p. 2). Towards this end, the identified variables and their indicators are defined, discussed and supported by theoretical assumptions to enable better replicability and reliability of the results (Lopes et al. 2019, p.3). It is important to note that the value judgements made with regards to the selection of variables and deterrence indicators that form the premise of the underlying arguments are also determined on the basis of empirical research conducted in academic fields where the scientific method is more rigorously applied, namely the field of electrical engineering more broadly, and computer science more specifically.

By limiting the study scope to only variables that are technical enablers, internal validity is also strengthened by avoiding potentially subjective assertions and arguments with regards to causal mechanisms that are related to contextual disciplines other than that of information security. Namely, crime is a complex behavioural phenomenon, with cybercrime imbuing significant additional complexity due to its inherent abstractness. However, the object of this study is not an explanatory approach seeking to determine causal mechanisms that are influencing DDoS crime rates, which would require the examination of the entire spectrum of deterrence. Since the aim is rather to contrast and compare the extent to which resistance and resilience factors are used to deter the identified technical enablers, the analysis allows for the exclusion of many variables that could otherwise play a role in the commissioning of DDoS attacks, for example financial or technological incentives.

While internal validity could potentially be increased by studying these deterrence factors on a single, more specific level of cyberspace abstraction (such as a study specifically looking into DNS based DDoS attacks for example), such a study would not ultimately contribute to a clarification of the stated research question. Namely, while deterrence on a single level of abstraction could in theory be full proof, the overall network could still remain equally vulnerable as attackers would favour a different attack vector, strategy or protocol.

3.6 Operationalization

The information security and data privacy controls discussed in chapter two are operationalized into positive resistance and resilience indicators in the table below:

Concept:	**Deterrence Indicator:**	**Targeting:**
Internet security is highly interdependent – Comparison category One	Digital hygiene	Gain probability, Loss value, Loss probability
	Layered defences	Gain probability, Loss value, Loss probability
	Security awareness	Gain value, Gain probability, Loss probability
	Capital allocation	Gain probability, Loss value
	Resource allocation	Gain probability, Loss value
	Administrative, physical and technical controls	Gain value, Gain probability, Loss value, Loss probability
Internet resources are limited – Comparison category Two	Availability requirements	Gain value, Gain probability
	Service Level Agreements	Gain value, Gain probability, Loss value
	Elasticity requirements	Gain value, Gain probability
	Data minimization	Gain value, Gain probability
Intelligence and resources are not collocated – Comparison category Three	Over-Provisioning	Gain value, Loss value
	Redundancy	Gain value, Loss value
	Risk assessments	Gain value, Gain probability

Accountability is not enforced – Comparison category Four	Third-party transfer requirements	Gain value, Gain probability
	Responsibility definitions	Gain value, Gain probability
	Consent	Gain value, Gain probability
	Processing limitations	Gain value, Gain probability
Control is distributed – Comparison category Five	Standardization of security and privacy controls	Gain probability, Loss value, Loss probability
	People, processes and technology	Gain value, Gain probability
	Third party obligations	Gain probability, Loss value, Loss probability
	Security incident procedures	Gain probability, Loss value
	Security incident reporting	Gain probability, Loss value

While negative indicators would have perhaps suited the research methodology better, as the research aims to identify the controls that mitigate the negative design aspects of the Internet, this would have been impossible due to the fundamental nature of the information security field. A famous quote by Eugene Spafford states that,

> *“The only system that is truly secure is one that is switched off and unplugged, locked in a titanium-lined safe, buried in a concrete bunker, and surrounded by nerve gas and very highly-paid armed guards. Even then, I wouldn't stake my life on it” (Bowen et al. 2002).*

Due to information security being a fundamentally risk-based practice, it is generally believed that no computer system can be 100% secure or ‘risk-free’, meaning that there is a potentially endless list of indicators that could negatively affect the security posture of the in-scope systems. For this reason, focusing on negative indicators would not constitute a feasible approach and would not lend much insight into the desired empirical inquiry.

The in-scope legislative documents will be assessed and examined for the presence of the above outlined positive indicators, whose contribution to the mitigation of the Internet’s flawed design will then be qualitatively discussed and compared between the two cases.

4.0 RESULTS

4.1 HIPAA 1996:

While HIPAA covers many general security controls, the undercurrent of the legislation is significantly biased towards the intended audience and the overall intended outcome of the legislation. As suggested by its title, HIPAA was not designed as an information security and privacy law in its own right, with security and privacy being only a part of the legislative act. The legislation covers a broad range of healthcare related topics within the U.S., including but not limited to health insurance coverage, healthcare information set standardization, medical spending guidelines and life insurance rules (HIPAA 1996, Pub. L. 104-191). The self-declared aim of the legislation was, among other things, to improve "the efficiency and effectiveness of the health care system" both in terms of PHI management, as well as with regards to the wider subject area (HIPAA 1996, Pub. L. 104-191 §261). For this reason, certain parts of the legislation in attempting to provide benefit to the industry as a whole steer away from potential security benefits, the most obvious of which are the repeated calls for administrative costs reductions for health care providers (HIPAA 1996, Pub. L. 104-191 §1172-4). Nevertheless, the legislation does give emphasis to the need for security policies and procedures to document and subsequently implement administrative, physical and technical controls to secure the confidentiality, integrity and availability of information systems and PHI (HIPAA 1996, Pub. L. 104-191 §1173). Furthermore, the legislation also emphasizes data transfer rules between various providers, both in terms of data format standardization, as well as controls standardization, more information on which is provided in the regulatory standard (HIPAA 1996, Pub. L. 104-191 §1173). Importantly, the regulation text defines 'systems' as pertaining to all components, including hardware, software, information, data, applications, communications and people – therefore encompassing people, processes and technology under its information security scope. Furthermore, all HIPAA requirements must be fulfilled by designated stakeholders who are assigned responsibilities and tasks for the development and implementation of the information security program (45 CFR §164.308, 2013). These stakeholders, as well as other employees of in-scope organizations, are also required to received security awareness training, albeit without any specification as to the frequency with which it should take place (45 CFR §164.308, 2013).

An important note with regards to HIPAA that should not be overlooked is naturally the age of the legislation itself. Having been written in 1996 it long pre-dates the widespread adoption or use of virtualization and cloud technologies, therefore it would be wrong to expect direct references or emphasis on such technologies. Nevertheless, as previously mentioned, in order to examine the regulations and standards that are required in order to comply with this legislation, the *Administrative Simplification* document of the U.S. HHS must be consulted. The first aspect of note within the HIPAA regulatory text is the so-called "Flexibility approach", which encourages in-scope entities to use any security measures deemed necessary to "reasonably and appropriately implement the standards and implementation specifications" as specified in the regulation (45 CFR §164.306, 2013). The regulation recommends the measures to take into account certain factors, including:

i. The size, complexity and capabilities of the entity;
ii. The technical infrastructure, hardware and software security capabilities of the entity;
iii. The costs of security measures; and
iv. The probability and criticality of potential risks to PHI.

(45 CFR §164.306, 2013)

Furthermore, each implemented control must be assessed for its effectiveness and suitability for the particular environment, including requiring the implementation of alternative security or risk mitigation measures where specific mandated controls are impossible to implement due to technical reasons or otherwise (45 CFR §164.306, 2013). While the kern of security best practices with regards to risk management and security operations is mandated by the regulation, including requirements for periodic risk assessment, risk mitigation, as well as security monitoring, the regulations are relatively lax in requiring the implementation of specific technical controls to the full extent. Namely, core security controls such as role-based access controls (RBAC), security monitoring, and data protection while mentioned, are more often than not required only broadly and not fully. In this sense, auditing and access log monitoring, protection of data in transit and at rest using encryption, password management, and malware protection are all optional requirements, i.e. recommended but not required (45 CFR §164.308, 2013). Furthermore, many administrative controls such as employee background checks, authorization and supervision procedures, access management policies and procedures are all mentioned but similarly optional controls (45 CFR §164.308, 2013). This implies that the requirement for DiD is also not achieved. While the legislation does require controls in all the pertinent categories, as well as requires PHI data isolation, it does not explicitly require boundary defence and only recommends encryption. Given the legislation's emphasis on cost efficiency, it is likely that a lack of such hard requirements results in many organizations omitting them from their information security management systems to better manage organizational and business costs, while still maintaining their HIPAA regulatory compliance.

The legislation nevertheless more stringently mandates requirements for redundancy in particular and business continuity management in general. For cases where damage to systems could occur, either physical (e.g. fire, vandalism, natural disaster, etc.) or logical (e.g. system failure, downtime from a DDoS attack, etc.) damage, the regulation demands a stringent application of business continuity processes, based on a predefined set of policies and procedures for responding to such emergencies (45 CFR §164.308, 2013). The implementation specification demands that PHI data is regularly backed up; a disaster recovery plan is created to outline the procedure for restoring system availability and mitigating data loss; a data and system criticality analysis is done to identify business critical data and system components; specific plans are maintained for the functional continuation and protection of critical business processes and components; and the above stated processes are required to undergo a continuous cycle of testing and evaluation (45 CFR §164.308, 2013). While specific data availability or system uptime requirements are not mentioned either in the regulations or the legal act, both documents often allude to the importance of maintaining this particular aspect of the C-I-A triad. Not being limited only to disaster related events, security incident management process requirements extend to all security incidents and anomalies for which clear procedures must be maintained covering specifications for the identification and mitigation of such events (45 CFR §164.308, 2013).

Apart from mandating information security and privacy controls, the legislation also sets considerable limitations on the collection, processing and sharing of PHI. The purpose limitation principle of HIPAA states that "a covered entity may use or disclose PHI for treatment, payment or health care operations" purposes, without requiring explicit consent or authorization from the individual who the information identifies (45 CFR §164.506, 2013). This use and disclosure limitation applies to cases in the administrative, civil and criminal legal spheres, unless "the action or investigation arises out of and is directly related to receipt of health care or payment for health care or action involving a fraudulent claim related to health; or if authorized by an appropriate order of a court…" (HIPAA 1996, Pub. L. 104-191 §248, p. 69). While explicit consent for the use and processing of PHI involving the above stipulated purposes is not required, consent is required for the sharing of PHI in relation to any activities not covered by the above, including for research purposes (45 CFR §164.508, 2013). For purposes other than treatment, payment and healthcare operations, the use, disclosure or sale of PHI is prohibited unless having received explicit authorization from the individual and adhering to a number of sub-requirements specifying the authorization process (45 CFR §164.508, 2013). Disclosure is also required upon request of the individual whom the PHI identifies, however it is not clear whether all data that is being collected, stored and processed must be revealed upon request (45 CFR §164.502, 2013). With regards to the principle of data minimization, there appear to be no legal or regulatory stipulations with regards to the amount, kind or extent to which the covered entities can collect, process and store PHI. However, the data minimization principle does apply to the sharing of PHI, mandating that only the bare minimum necessary information be shared, as required for the completion of treatment, payment or health care operations purposes (45 CFR §164.502, 2013). In addition, any shared information must be anonymized prior to its disclosure. If healthcare data is anonymized it is no longer considered to be PHI, as per §164.502 of the regulation (45 CFR §164.502, 2013). Nevertheless, all PHI data transfers to third parties are subject to the provisions of the HIPAA regulations, requiring all third parties to apply and guarantee like security and privacy controls, as well as requiring a written agreement documenting the purposes, assurances and protection that is to be afforded to PHI, prior to it being provided (45 CFR §164.508, 2013). Third parties are furthermore required to report any breaches of PHI to the primary controller of the information (45 CFR §164.314:164.410, 2013). While data breaches must always be documented, data breach reporting to the regulatory authority is required for all holders of PHI when the breach involved 500 or more individuals (45 CFR §164.410, 2013). The report can be filled no later than 60 days after the discovery of the breach (45 CFR §164.408, 2013).

While patch management is implicitly alluded to by certain requirements such as that of risk management and malware protection, it is not explicitly stated presenting a significant gap in the security framework. While one could argue that the risk management process would include mitigation of the identified risks and vulnerabilities, such mitigation does not necessarily require patching but can mitigate issues by other means, which could result in entities not having to patch while still maintaining compliance with HIPAA security and privacy rules.

4.2 FISMA 2014:

Although the latest and current version of FISMA was passed into law in 2014, the legislation was initially introduced as part of a broader E-Government Act of 2002 (Ross et al. 2005, p.864). The legislation acknowledged the growing importance of information technology in general, and information security in particular, to the U.S. national economy, and targeted the creation of an enhanced and more secure system for information access (Ross et al. 2005, p.865; White 2010, p.372). In this regard, the stated objective of the legislation is to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets" (FISMA 2014, 44 USC §3551). Similar to the HIPAA, FISMA focuses on protecting the three core elements of information security, including confidentiality, integrity and availability through a risk management approach and on the basis of codified information security policies, procedures, principles, standards and guidelines (FISMA 2014, 44 USC §3552-§3553). While the legislation is generally applicable to all federal information and information systems, certain elements are explicitly outside of its scope, namely information and systems operated by the U.S. Department of Defence as well as the "intelligence community", an umbrella term for intelligence and security agencies of the U.S. federal government (FISMA 2014, 44 USC §3553). For all other information and systems not included in these two categories however, the oversight and regulatory authority has been given to the U.S. Department of Homeland Security, even though the roles and responsibilities for implementing various mandated measures, controls and programs are assigned to a variety of actors, which can be found in Appendix 1.

The legislation sets out to mandate the creation of a risk based approach to information security and data privacy throughout the federal government, stating that the protections embedded in the policies and procedures should be "commensurate with the risk and magnitude of the harm" posed to the specific systems and information in question (FISMA 2014, 44 USC §3554). Each government agency or other in-scope institution is therefore to develop and maintain its own information security program, tailored and designed to meet the information protection needs and reduce the risks that are periodically identified and specific to that agency's systems and information (FISMA 2014, 44 USC §3554). A point of significance is also the important role assigned to NIST, which is tasked with creating the standards and guidelines for the effective management of information security and privacy (FISMA 2014, 44 USC §3553). As one of the foremost authorities with regards to information security and general information technology standards, its persistent role in the legislation provides the in-scope institutions with a state-of-the-art knowledge centre on which they can rely on.

Moreover, the legislation touches on many relevant aspects of information security directly. A clear requirement for proper resourcing and responsibility distribution, including staffing of information security personnel, training, managerial designation and budget allocation is mandated, as required in order to mitigate the identified risks (FISMA 2014, 44 USC §3554). While the document does allude to cost-effectiveness, it stresses the importance of applying security controls throughout the lifecycle of every information system, including minimally acceptable system configuration standards, and minimal controls for networks, facilities, people and systems or groups of information systems, as appropriate (FISMA 2014, 44 USC §3554). As such, the legislation spans the administrative, technical and physical control domains in the categories of people, processes and technology, relying on NIST and the specific information security program to further tailor these as required by each institution's specific information protection needs. The mandated NIST standards were published under Special Publication 800-53 (currently at rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations*[6]. A clear requirement is also placed on the implementation of patching and overall maintenance of digital hygiene by requiring "a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies" in the information security program or systems (FISMA 2014, 44 USC §3554).

While the FISMA law is relevant in its own right, for the purposes of this study the FedRAMP program deserves particular attention. In 2011 the U.S. Office of Management and Budget, through the authority vested to it by FISMA, published a policy memo for the creation of the FedRAMP Program, which aimed to create a process for authorizing the adoption and use of cloud services by the federal government (Van Roekel 2011, p.1). The stated aim of the program was to respond to the need for the federal government to ensure the "security, interoperability, portability, reliability and resiliency" of its information systems by providing a federal policy and security benchmark for the acquisition of cloud services (Van Roekel 2011, p.1-2). The memorandum further applies to the following:

1. Executive departments and agencies procuring commercial and non-commercial cloud services for their information systems, including those agencies' contractors, third parties and other subordinates;
2. All cloud deployment models (i.e. Public Clouds, Community Clouds, Private Clouds and Hybrid Clouds);
3. All cloud service models (i.e. Infrastructure as a Service, Platform as a Service, and Software as a Service).

(Van Roekel 2011, p.2).

Nevertheless, a footnote of the memorandum does provide exemption from FedRAMP requirements for departments that select a private cloud deployment model, implement the private cloud fully on premise (i.e. within a federal facility), and do not provide cloud services to external entities (Van Roekel 2011, p.2). Such environments are nonetheless still required to fully comply with FISMA and the adjoining NIST security standards and guidelines for private cloud deployment models.

At its core, the FedRAMP program is an accreditation based program. The memorandum established the Joint Authorization Board (JAB), whose task is among other things, to accredit third party assessment organizations (3PAOs) who then "provide independent assessments of CSPs' implementation of the FedRAMP security authorization requirements" (Van Roekel 2011, p.3). The accreditation process for 3PAOs involves an examination of these organizations' technical and other competencies on the basis of ISO/IEC standards, to determine whether they are competent to carry out authorization assessments (Van Roekel 2011, p.3). The authorization process intended not only to harmonize the security and privacy controls implemented in federal cloud solutions and services, but also to further enable federal entities to make use of standard contractual language and service level agreements (SLAs) (Van Roekel 2011, p.4). This ultimately allows the federal government to create a uniform level of service guarantees in all cloud solutions and services it uses, regardless of vendor, deployment or service model, system or environment.

[6] Full standard is available at: https://nvd.nist.gov/800-53.

At the time of writing, there are 210 FedRAMP authorized cloud solutions available on the American marketplace[7].

While a full assessment of the FedRAMP program is out of scope of this research paper, determining the full extent of FISMA's requirements in relation to the identified positive indicators cannot be done without examining the NIST SP 800-53 rev. 4 and the controls required therein. The standard contains a plurality of controls sorted into the following control families:

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

The controls are further sorted into low, medium and high impact controls. Each control contains control enhancements, i.e. sub-controls, as well as process guidance for the effectiveness assessment of each control (Joint Task Force Transformation Initiative Interagency Working Group 2014, p.10). This is furthermore in line with the FISMA requirement for "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices," including the implemented security and privacy controls (FISMA 2014, 44 USC §3554). Even once authorized, CSPs must still commit to a process of regular monitoring and validation of the controls in place, which involves the provisioning of compliance evidences to the appropriate agencies and stakeholders.

The standard mandates the implementation of layered defences following the concept of defence-in-depth specifically, as well as secure architecture requirements more broadly (Primary control PL-8; related controls CM-2, CM-6, PL-2, PM-7, SA-5, SA-17). Availability and redundancy requirements also feature prominently throughout the standard, the latter mainly under the Contingency Planning control group. Apart from general resource availability requirements (SC-6), the in-scope organization is also tasked with

[7] For full list see https://marketplace.fedramp.gov.

ensuring the availability requirements of its primary and backup providers and locations through service level agreements; create priority-of-service clauses where these are necessary for the functional continuation of (critical) components; and include recovery time objectives for all processes (CP-7 and CP-8). Unlike the HIPAA regulation, the standard also includes a control (SC-5) with three sub-controls specifically intended for denial of service protection. These include measures to prevent the launching of (D)DoS attacks from internal systems, including egress filtering, arbitrary transmission restrictions, resource limitations, as well as restrictions for acquiring and installing (D)DoS software. Furthermore, over-provisioning is also required, both in terms of system capacity, bandwidth, and other viable redundancies (SC-5.2). There appears to be no specific mention of elasticity requirements. While there are considerable limitations imposed on information flows (AC-4), there are no controls requiring data minimization, processing limitations or consent for data processing. Nevertheless, processing control agreements are required when sharing or querying data external to the organization's native system (AC-20).

The legislation furthermore requires each in-scope entity to maintain security incident management policies and procedures, including reporting requirements and special sub-requirements for major incidents (FISMA 2014, 44 USC §3558). All security incidents in federal systems must be reported to the US-CERT with one hour, while major incident reports must be made available to Congress within seven days following the detection of the incident (FISMA 2014, 44 USC §3558; Cybersecurity and Infrastructure Security Agency 2017, p.1-2). The incident management program must also extend to include plans and procedures specifically for operations continuity and disaster recovery (FISMA 2014, 44 USC §3558). In an effort to improve the incident management process not only on an individual agency basis but nationally, the legislation also mandated the creation of a Federal information security incident centre (FISMA 2014, 44 USC §3556).

While neither FISMA nor the NIST guidelines specifically mention third-party transfer requirements in the sense of third-party data hosting, the juridical definitions as set by the legislation demand that equal requirements be placed on all parties hosting federal data. The legislation namely does not determine the scope of its applicability only by institutions but also by data, therefore the requirements are extended to any system that hosts federal information, regardless of whether these systems are hosted or owned by a federal entity or not. Furthermore, additional personnel security requirements are mandated for third parties interacting with federal information systems or data, as outlined by NIST control PS-7. These include but are not limited requirements for the definition of roles and responsibilities, security controls, incident notification, compliance monitoring, as well as security training and awareness, all of which are required for all systems and institutions under FISMA's scope (PS-7; FISMA 2014, 44 USC §3554).

4.3 GDPR 2016:

Among the legislative documents being analysed in this paper, the GDPR is likely the most publicized and known. Being among the first such extensive and broad regulations of its kind, it drastically changed the rules, norms and regulatory perspectives on the issues of data privacy specifically, and by extension also information security more broadly (Lopes et al. 2019, p. 1). The GDPR is a data focused regulation, in that its material scope, as defined by Article 2, extends only to personal data, i.e. personally identifiable information (PII), defined as "any information relating to an identified or identifiable natural person ('data subject')" who is an EU citizen and also, or by extension, located within EU territory (Regulation 2016/679/EU, p. 33). While this implies that the regulation does not by default regulate any particular person, institution, or other legal entity, it nonetheless directly applies to an immensely broad range of natural and legal persons, agencies, public authorities, institutions and other bodies, with respect to the nature of their data processing and in line with their professional and commercial activities (Regulation 2016/679/EU, p.3:32). The broad material scope combined with the hefty fines that are mandated for cases of non-compliance understandably created quite a stir globally as companies scrambled to implement the required contents of the regulation before it was due to take effect (Voss and Houser 2019, p. 289).

While not an information security law within its own right, data privacy and data security are often interrelated points of focus. Although dependent on the context, the notion of privacy tends to frame private data in terms of its informational value to the individual it represents. As such, it is sometimes referred to as a "controlled disclosure", where a subject him or herself chooses what personal data is appropriate to reveal (Pfleeger et al. 2015, p.589). For this reason, privacy as such is arguably a more subjective phenomenon than information security, as each individual must themselves determine what they consider as sensitive personal information that should remain of a private nature, and which personal information (if any) should be deemed of a public nature. For this reason, privacy as a concept long predates the field of information security, in terms of its association with the protection of digital information and computer systems and has more often been framed through legislative undertakings rather than technical documents or standards. This is quite evident in the GDPR's main body of text that is composed of long and explanatory sentences organized into articles and paragraphs, different from the FISMA for example that often displays very short and to the point sentences with keywords relevant to information security. Furthermore, while often alluding to the traditional concept of C-I-A, the GDPR more often frames requirements in line with the objective of protecting the "rights and freedoms of natural persons" as opposed to the protection of systems (Regulation 2016/679/EU, p.48). A closer examination of Articles 37 and 39 regarding the creation of the Data Protection Officer (DPO) position also puts emphasis on personal qualities and qualifications that are more in line with a legal background, as opposed to a background in computer science or an IT security qualification (Regulation 2016/679/EU, p.55-56). The DPO is further responsible for many of the administrative duties required by the GDPR, such as carrying out mandatory security and privacy awareness training campaigns (Regulation 2016/679/EU, p.56). Similarly, as opposed to the usual mix of administrative, physical and technical controls recipe for information and data protection, the document rather focuses on "technical and organizational" measures, reaffirming its legal as opposed to IT orientation (Regulation 2016/679/EU, p.5). Nevertheless, as the GDPR applies to all PII, not only electronic PII, the requirements and controls also extend to the physical domain that appears absent from the "technical and organizational" measures definition, making little practical difference in terms of the required control domains.

Nevertheless, in keeping with its reputation, the document contains some very stringent rules with regards to the security of personal data. Grounded in a risk based approach, the legislation stipulates a number of core principles, concepts and practices as foundational requirements for PII processing, the majority of which are enshrined in Article 5 (Regulation 2016/679/EU, p.15:35).

Article 5	
Principle:	**Description:**
Lawfulness, fairness and transparency	All personal data processing must be done on a lawful basis, in fairness towards the data subject and in a transparent manner, both towards the regulatory authority, as well as to the data subject.
Purpose limitation	All personal data processing must be done only for the intended purposes and not exceed the limits thereof.
Data minimization	All personal data collected and processed is "adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed."
Accuracy	Efforts should be made to maintain the accuracy of personal data and in cases where found to be inaccurate, data should be erased or rectified accordingly and without delay.
Storage limitation	All personal data should be collected, stored and retained only as necessary to achieve the purposes for which the data is processed.
Integrity and confidentiality	All personal data should be kept secure, protected against unauthorized access, as well as against "accidental loss, destruction or damage."

(Regulation 2016/679/EU, p.35-36).

While many of the principles are directly related to traditional information security practices, the GDPR associates the purpose limitation principle as specifically important to the guaranteeing of the confidentiality, integrity and availability of information and for the prevention of data breaches, hacks, accidental disclosures, as well as other events such as denial of service attacks (Regulation 2016/679/EU, p.9). All processing of PII should be predisposed to a continuous process of risk and impact assessment to identify threats to data subjects and implement appropriate mitigating measures (Regulation 2016/679/EU, p.15-16). Furthermore, Article 32 is specifically dedicated to the security of personal data and its processing. While absent any specific availability requirements, redundancy procedures or service level agreements, the regulation stipulates that availability and access to personal data must be restored "in a timely manner" in the event of an availability incident (Regulation 2016/679/EU, p.52). The mandated technical and organizational controls are further required to undergo a continuous process of assessment and testing, following stipulated codes of conduct that are referred to in Article 40 (Regulation 2016/679/EU, p.52).

Some other notable concepts introduced by the GDPR include data protection by design and by default, effectively mandating that data protection measures and principles enshrined within the GDPR be mandatorily included as a default aspect of any system or data processing design (Regulation 2016/679/EU, p.48). This does not include specific requirements for defence-in-depth however, which would thus be a design decision left to the individual system architects. The legislation generally does not go into information security specifics, also making no mention of required system patches or updates or over-provisioning of resources. With regards to more general demands for resource provisioning, the regulation clearly and extensively documents the requirements thereof. As a European regulation, the document necessarily mandates that the member states dedicate a sufficient level of capital, human, infrastructural and other resources to enable the supervisory authorities and other supporting bodies to effectively carry out their responsibilities (Regulation 2016/679/EU, p.22). Furthermore, the allocation of both capital and other resources is namely deriving from the responsibilities of the data controller[8]. The data controller must ensure that any processing[9] done on their behalf by a data processor[10] must ensure sufficient guarantees "in terms of expert knowledge, reliability and resources to implement technical and organization measures, which will meet the requirements of this Regulation, including for the security of processing" (Regulation 2016/679/EU, p.16). While reliability could be considered an aspect of redundancy, the document does not clarify what kind of reliability it is referring to; therefore suggesting that the term here refers to the reliability of the processor as an actor. Responsibility, accountability and liability allocation is also underlined throughout the Regulation, particularly in Articles 24 ('Responsibility of the controller') and 28 ('Processor') (Regulation 2016/679/EU, p.47-49). Similar to other parts of the Regulation, Article 24 mostly focuses on controls geared towards preventing infringements of the rights and freedoms of data subjects as opposed to the requirements of C-I-A.

With regards to data transfer requirements, the GDPR contains a number of articles and clauses that outline the mechanisms and requirements for data transfers, these being considered some of the most stringent in the world at the time of writing. In addition to complying with all the requirements as applicable to a (co)controller or a processor in Articles 24 and 28, a controller must also guarantee a legal basis for the transfer of all PII to other legal jurisdictions and entities. Namely, pursuant to Article 45, the European Commission (EC) may authorize such transfers to take place on the basis of an adequacy decision, which legally satisfies the requirement for an adequate level of protection within the legal jurisdiction for which the data is destined (Regulation 2016/679/EU, p.61). If such an adequacy decision is absent, Article 46 allows the data controller a number of other means, including standard contractual clauses, binding corporate rules, and other binding and enforceable agreements that allow for the enforcement of equal standards in non-European jurisdictions (Regulation 2016/679/EU, p.62). In the absence of the ability to monitor and enforce equal data protection standards, data transfers between entities or jurisdictions are not allowed, and the controller will be held liable for any such illegitimate breaches. Prior to any PII collection or processing, explicit consent is also required from the data subject,

[8] A 'controller' is defined as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Regulation 2016/679/EU, p. 33)

[9] 'Processing' "means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (Regulation 2016/679/EU, p. 33)

[10] A 'processor' is defined as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Regulation 2016/679/EU, p. 33)

thus there are a number of layers of controls with regards to the legitimacy of collecting, processing, transferring and storing of private data (Regulation 2016/679/EU, p.37).

As part of Article 32 mandating the security of data processing, the GDPR also stipulates that controllers and processors must be prepared and able to restore availability of their systems and data after a physical or technical incident (Regulation 2016/679/EU, p.52). With regards to security incident reporting, after becoming aware that a data breach has taken place, the controller or processor is required to inform the supervisory authority within 72 and will be held liable if appropriate incident management processes were not implemented (Regulation 2016/679/EU, p.52).

4.4 NIS 2016/Wbni 2018:

The EU Directive on the Security of Network and Information Systems in the Netherlands was passed into law as the *Wet beveiliging netwerk- en informatiesystemen* (Network and Information Systems Security Act) on 17 October 2018. The directive aimed to provide a supplementary legal framework to the GDPR, with a more data neutral scope to expand the applicability of security best practices within the EU beyond only PII (Cole and Schmitz-Berndt 2019, p.3). One of the primary aims of the legislation is to "limit the failure of availability or the loss of integrity of network and information systems", therefore ensuring the continuity of services offered by vital service providers specifically, as well as digital services providers more generally (Art. 3 Wbni, 2018; Ministerie van EZK 2018, p.3). While the directive provided a set of criteria for the definition of a vital services providers (see Appendix 2), it was ultimately up to the national legislators to decide exactly which services would be included in these categories (Cole and Schmitz-Berndt 2019, p.3). The designated were intended to include service providers that are heavily reliant on ICTs and that are essential to the economy of the Member States, as well by extension to the EU single market as a whole (Cole and Schmitz-Berndt 2019, p.3). Due to their significance to the continued functioning of many European businesses, search engines, cloud computing services and online marketplaces were identified as key digital service providers uniformly across the EU by the directive (Directive 2016/1148/EU, p.30; Ministerie van EZK 2018, p.3; Cole and Schmitz-Berndt 2019, p.3). In spite of this uniformity, not all such providers are regulated under these rules, as digital service providers with fewer than 50 employees and less than 10 million Euros in revenue or assets are exempt from the requirements (See Appendix 3).

Based on the guidance provided by the EU on the categorisation of vital services providers, the Dutch legislation dedicated different competent authorities responsible for each sector. The digital services sector, under which also CSPs are classified, was placed under the responsibility of the Dutch Ministry of Economic Affairs and Climate, which in 2018 published a guidance document for the implementation of the new legislation within this sector (Ministerie van EZK 2018, p.3). According to the document and stated in more legal terms, digital service providers are tasked with two primary duties, a duty to report cyber related incidents[11] to the regulator (*Agentschap Telecom*), and a duty of care for their systems and networks in terms of organizational and technical measures for information security, protection of data and the minimization of likelihood and impact of incidents (Ministerie van EZK 2018, p.3). Furthermore with respect to CSPs, the document states that while all cloud deployment and service models are in-scope, private clouds that are used exclusively inside an organization would not fall under the rules and regulations of the Wbni (Ministerie van EZK 2018, p.6).

The primary responsibilities with regards to information security controls are outlined in Articles 7, 8 and 9, and require an in-scope provider to "take appropriate and proportionate technical and organizational measures to control the risks to the security of their network and information systems" (Art. 7 Wbni, 2018). Mandating a risk-based approach, the legislation lays out the national strategy for the security of networks and information systems by requiring that at the minimum the following points be implemented following industry best practices:

a. The security of systems and facilities;
b. Handling of incidents;
c. Business continuity management;
d. Monitoring, control and testing;
e. Compliance with international standards.

(Art. 7 Wbni, 2018)

The legislation furthermore puts clear emphasis on security incident management, notification and reporting. The directive mandated that each Member State establish, resource and designate computer security incident response teams (CSIRTs), within a hierarchical structure of competent authorities that are to intervene, assist, inform and support institutions during security incidents (Directive 2016/1148/EU, p.17). Towards this end, Articles 10 through 16 of the Wbni are fully dedicated to the establishment of rules surrounding the incident notification, reporting , investigation and management processes for the purposes of ensuring sufficient business continuity capabilities among the in-scope service providers (Art. 10-16 Wbni, 2018). Incidents that are found to have "significant consequences" on the services provisioning of the provider require notification to the regulator at all times (Ministerie EZK 2018, p. 9). This is determined on the basis of the number of affected users, the duration of the incident, and the size or geographic extent of the effect (Art. 10 Wbni, 2018). While the legislation contains extensive clauses regarding the control that is to be exercised over the collection and processing of incident related information by CSIRTs and the competent authorities, the law nonetheless mandates the free disclosure of incident information and data if that is necessary for incident resolution or in the general public interest (Art. 23 Wbni, 2018).

Simultaneously, the legislation never specifically determines how or to what extent any of the risk mitigation controls should be implemented, which was identified by the EU as a gap that was subsequently mitigated with the publishing of the Implementation Regulation EU 2018/151 (Ministerie EZK 2018, p. 11;

[11] An 'incident' is defined as "any occurrence that has a damaging effect on the security of network and information systems" of the service provider (Ministerie van EZK 2018, p.9).

Commission Implementing Regulation (EU) 2018/151). Although declaring that service providers are free to determine themselves what kind of administrative, technical and physical controls are considered appropriate and proportional to their environment and its risk posture, certain elements are explicitly required, including:

- Security policies and procedures covering at least information security management system, risk analysis, human resources, security operations, security architecture, system life cycle management and cryptography;
- Availability, in terms of both physical and environmental security, to prevent all instances of system failure, including through human error, malicious activity or natural disasters;
- Critical supplies and suppliers management to ensure the accessibility, replaceability and traceability of critical system components;
- Access management in terms of both physical and logical access points;
- Monitoring and detection of anomalous network and system behaviour;
- Vulnerability management, including vulnerability mitigation and patching;
- Contingency planning, including disaster recovery sites, redundant components, and regular exercises and testing thereof.

(Commission Implementing Regulation (EU) 2018/151, p. 49-50).

While the text does cover people, processes and technology, it nonetheless leaves much up to the discretion of the service provider. Administrative controls such as the development of skills and implementation of trainings are thus mentioned but not required (Commission Implementing Regulation (EU) 2018/151, p. 48). Similarly, there is no mention of mandatory resource or capital provisioning for the implementation of the controls. Nonetheless the Implementation Regulation emphasizes security architecture requirements related to DiD, including the segregation of networks and systems, including data and critical system isolation, and the broad use of encryption (Commission Implementing Regulation (EU) 2018/151, p. 48-49).

While not explicitly mentioning service level agreements, the extensive requirements and controls intended to secure the risks posed by suppliers and third parties, particularly in terms of accessibility, replaceability and traceability of critical system components, suggest that companies must implement SLAs or generate equivalent legal and contractual instruments. Nevertheless, while covering the supplier engagements quite extensively, the Wbni or the supplementary regulatory documents do not specifically outline security requirements pertinent to data sharing and system interaction with third parties or other externals, leaving a considerable gap in the legislation. Although a service provider governed by Wbni/NIS requirements would still be held liable if a security incident resulted due to compromise of third-party systems, there are no specified controls or requirements for mitigating such an eventuality. Responsibility distributions, either internal to an organization, or external in the context of third-party engagements are similarly not covered. Due to the data neutral composition of the legislation, many of the data specific requirements are also missing. Processing limitations, data minimization and consent mechanisms are therefore not required. Furthermore, there is also no specific emphasis on virtualization technology controls, therefore there is no mention of over-provisioning or elasticity requirements.

The Implementing Regulation further requires that business continuity measures be implemented on the basis of pre-defined availability criteria that are acceptable to the service delivery level of the provider (Commission Implementing Regulation (EU) 2018/151, p. 50). Interestingly, while Article 7 of the NIS requires that the national strategies implement security awareness raising and training campaigns, this is entirely absent from the Wbni, which makes no such mentions or requirements (Directive 2016/1148/EU, p.16). Interestingly also, while referring to mitigating measures when identifying risks to a network and systems, the legislation or regulatory documents do not make any mention of patching or system updates.

4.5 Results Table:

Concept:	**Deterrence Indicator:**	**HIPAA:**	**FISMA:**	**GDPR:**	**NIS:**
Internet security is highly interdependent – Comparison category One	Digital hygiene	No	Yes	No	No
	Defence-in-depth	No	Yes	No	Yes
	Security awareness	Yes	Yes	Yes	No
	Capital allocation	No	Yes	Yes	No
	Resource allocation	Yes	Yes	Yes	No
	Administrative, technical and physical controls	Yes	Yes	Yes	Yes
Internet resources are limited – Comparison category Two	Availability requirements	Yes	Yes	Yes	Yes
	Service Level Agreements	No	Yes	No	Yes
	Elasticity requirements	No	No	No	No
	Data minimization	No	No	Yes	No
Intelligence and resources are not collocated – Comparison category Three	Over-Provisioning	No	Yes	No	No
	Redundancy	Yes	Yes	No	Yes
Accountability is not enforced – Comparison category Four	Risk assessments	Yes	Yes	Yes	Yes
	Third-party transfer requirements	Yes	Yes	Yes	No
	Responsibility definitions	Yes	Yes	Yes	No
	Consent	Yes	No	Yes	No
	Processing limitations	Yes	No	Yes	No
Control is distributed – Comparison category Five	Standardization of security and privacy controls	Yes	Yes	Yes	Yes
	People, processes and technology	Yes	Yes	No	Yes
	Third party obligations	Yes	Yes	Yes	No
	Security incident procedures	Yes	Yes	Yes	Yes
	Security incident reporting	Yes	Yes	Yes	Yes

5.0 DISCUSSION

While the results section identified the presence and absence of the positive indicators within each legislative document, the following section will examine a number of other relevant aspects that should be taken into account to create an accurate comparison between the two cases.

5.1 Regulatory Model

The cases and documents under study differentiate significantly, not only in terms of their scope and breadth, but also in terms of their regulatory models, legal systems, applicability, and jurisdictional delimitation. Firstly, the NIS and the GDPR are two fundamentally distinct pieces of European legislation. Namely, a European directive is a legislative act that defines the desired outcomes that must be achieved by all EU member states but is not transcribed directly into member state national law (European Union 2020). It is therefore at the discretion of the individual member states to determine how these outcomes will best be achieved, modifying and supplementing their respective national legislation, as well as designating the regulations and a regulator in accordance with the aims of the directive (European Union 2020). In the context of the Netherlands therefore, the actual legislative basis for the provisions of the NIS, as earlier mentioned, is the Dutch national *Wet Beveiliging Netwerk- en Informatiesystemen* (Wbni).

As mandated by Article 8 of the NIS Directive, the Wbni designates different competent authorities that are tasked with monitoring and regulating the implementation of the Wbni legislation across the in-scope sectors and organizations (Art. 4 Wbni, 2018). As each competent authority is responsible for defining its own regulations and acceptance criteria for the implementation of the law, especially with regards to the security and privacy controls pertinent to Article 7 of the Wbni, these criteria might diverge depending on the sector (Art. 7 Wbni, 2018). Nevertheless, obtaining said guidance and implementation information in a manner deemed sufficient was quite a challenging task. While the European Commission did issue the Implementation Regulation 2018/151 to offer supplementary guidance on the implementation of the NIS Directive in general, the Dutch Ministry for Economic Affairs and Climate further as the relevant competent authority, issued the implementation guidance document for digital services providers, both of which were included in the analysis. Unlike the NIS Directive however, the GDPR as a European regulation is a binding legislative act whose contents must be applied uniformly by all EU member states, including the Netherlands (European Union 2020). For this reason, the legislation contains specific clauses that outline and warrant specific regulatory requirements, therefore not requiring additional legislation or regulations for the implementation of the rules. Although Article 51 of the GDPR mandates the creation of supervisory authorities within the EU member states, these institutions are tasked with ensuring a “consistent application of this Regulation throughout the Union”, as opposed to creating regulations themselves (Regulation 2016/679/EU, p. 65).

On the other side of the spectrum, the United States Code (USC) contains general and permanent federal laws that were passed by the U.S. federal government. It does not however include the regulations, decisions and laws issued by federal courts, federal agencies, treaties and state or local governments (Usa.gov 2020). For this reason, the FISMA and HIPAA fundamentally differentiate from the GDPR and Wbni in that they do not contain many specific regulations that are to be implemented as a result of these legislative acts, but provide the authority and responsibility for doing so to the relevant ministry ('secretary') or agency. In this manner, Sec. 264 of Public Law 104-191 (HIPAA) therefore tasks the U.S. Secretary of Health and Human Services to create detailed recommendations on security and privacy standards for PHI (HIPAA 1996, Pub. L. 104-191, §264, codified as amended at 42 USC 1320d-2). For this reason, the results included information retrieved from the HIPAA Administrative Simplification Regulation Text published by the U.S. Department of Health and Human Services to ascertain the specific nature of the security and privacy controls required by the legislation. Codified under section 164, the HIPAA Privacy Rule and HIPAA Security Rule as they became known, set the technical and non-technical federal standards that are required for the protection of (electronic) PHI (Office for Civil Rights 2013). In the same manner, the analysis of FISMA included the regulatory documents published by the OMB, GBA and NIST, including the specifics related to FedRAMP.

Considering the above stated, one would expect the US federal legislation to be vaguer than its Dutch equivalent, however in general this did not appear to be the case. In this context it is also important to note that the Dutch and American legal systems follow two different forms of jurisprudence, the prior being based on the civil law tradition, while the latter on the common law tradition (Syam 2014). While these distinctions are not always clear-cut and certainly more intricate than this basic description would suggest, the relevance of this difference to the research paper at hand lies with the fact that common law more heavily relies on case law through which the contents of legislation is interpreted and potential ambiguities resolved (Syam 2014). Nevertheless, the American legislation more clearly defined the requirements from the start, aligned them with information security best practices, and established the necessary supporting documents to enable their correct interpretation. Especially the NIS in this sense lacked any clear guidance on the manner in which security and privacy controls should be implemented. The Wbni's codification of the directive also did not include any nuances or additional insights to improve the information security management system of the in-scope entities. Furthermore, it did not supplement the legislation with sufficient ancillary documentation to enable an effective, coherent and standardized implementation of deterrence strategies that would allow in-scope entities to go beyond its prescriptive wording and gain value from its guidance. An intricate point of consideration in this regard is also the role of the technical supporting agencies, these being the NIST in the US and ENISA in the EU. While ENISA did publish guidelines to support the implementation of minimum security measures for DSPs following high-level NIS requirements, these guidelines are nowhere prescribed, required or recommended by either NIS, the Wbni or any of the supporting documentation. For this reason, it would be incorrect to take these guidelines into consideration in equal measure as those of the NIST SP 800-53. FISMA on the other hand conveys the responsibility for the maintenance of security policies and procedures to the Directors of the federal agencies that are in scope of the legislation (FISMA 2014, 44 USC §3553). It furthermore delegates the development of standards and guidelines to the NIST which the in-scope organizations are explicitly required to implemented (FISMA 2014, 44 USC §3553). As the FISMA legislative act itself is relatively short, yet the scope and breadth of its coverage is extensive, it necessarily requires delegation to, engagement with, and participation of numerous federal actors to drive its implementation, a point of reference that would've been beneficial to the NIS Directive as well. In this regard, while the directors of the federal agencies are responsible for implementing cyber security programs, other duties are delegated to other government institutions, as listed in Appendix 1 (Office of Management and Budget 2019, p.6-7).

5.2 Applicability

Due to the varied nature of the legislative documents being assessed, their regulatory requirements also apply differently and variedly to various actors and institutions, as well as to different forms of information. While FISMA and HIPAA are both federal pieces of legislation, their applicability varies widely. HIPAA being a data oriented legislation, was designed specifically to regulate the healthcare industry, therefore the applicability of the mandated standards extends to "covered entities" which include:

1. A health plan;
2. A health care clearinghouse;
3. A health care provider who transmits any health information in electronic form.

(HIPAA 1996, Pub. L. 104-191, §1172, codified as amended at 42 USC 1320d-1).

The applicability clause was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 to extend the "Application of security provisions and penalties to business associates of covered entities" (HITECH 2009, secs. 13401, Pub. L. 111-5, 123 Stat. 227). HIPAA's provisions regarding information security and data privacy relate specifically to PHI, therefore rendering any institution that does not fit the description of a covered entity or handles PHI out of scope. Similarly, the material scope of the GDPR is data specific and extends only to PII as such, and not any specific institutions (Regulation 2016/679/EU, p. 32). Article 2 of the GDPR states that

> *"This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"*

(Regulation 2016/679/EU, p. 32).

FISMA on the other hand, applies to any and all information and information systems that support Federal operations and assets, while the NIS directive applies to operators of essential services and digital service providers, as per the definition in Article 1 of the law (FISMA 2014, 44 USC §3551; Art. 1 Wbni, 2018). A full list of what the European Council identifies as operators of essential services is identified in Annex II of the Directive (see Appendix 2). Furthermore, Article 3 of the Wbni also alludes to similar requirements being applied to national service providers as well (Art. 3 Wbni, 2018).

While the data that was collected allows for a quality analysis of the research subject, the selectiveness of the data nonetheless presents certain methodological problems for the results. While looking at Federal and National legislation, as well as supporting documentation such as regulatory texts, presents a clear picture of the high-level requirements, the omission of much other legislation that relates to information security and data privacy indirectly – including state or local legislation, case law, executive orders, etc. – necessarily creates a gap in the results (Bowen 2009, p.32; Yin 2009, p.80). This document selectivity bias could have been avoided by expanding the scope of the research to include more ancillary legislation, however this would not have been feasible given the scope and time limitations of this research paper. Specifically in relation to the omission of case law, precedents, legal interpretations and other guiding decisions, the research also necessarily displayed a certain measure of researcher bias, as the exclusion or inclusion of certain positive indicators was done on the basis of the researcher's own interpretation of the legal texts, as opposed to relying on the interpretation of legal experts and *stare decisis*, i.e. legal precedents. Nevertheless, in terms of feasibility, such a method would likely have encountered a lack of supplementary data due to the short period of time that the GDPR and NIS have been in effect, offering little in terms of legal precedents, cases and evidences.

While this is necessarily the case to a certain extent, the research and methodological decisions were nonetheless guided by exemplified legal and academic texts to arrive at impartial and logical conclusions. In this sense, certain results, such as FISMA's lack of controls requiring data minimization, processing limitations or consent for data processing, must also be approached critically from the perspective of the processor and within the context of the earlier explained. Since the legislation relates to government data processing, they do not necessarily require these mechanisms due to their privileged nature for viewing citizens' data. This is also the case with the GDPR that government institutions are exempt from it in some cases. However, since data minimization is not enforced on any level, it does mean that inter-agency processing is made easier, meaning that data collected for sanitation could also end up being processed by the DHS, thus lowering privacy controls in the long term.

The varied applicability and scopes of the legislative documents necessarily render a proportion of the results up to interpretation, particularly in relation to the standardization indicator. While all four pieces of legislation standardize the controls they require across the in-scope institutions, these institutions nonetheless vary widely. As a result, it is difficult to assert whether the standards required by these laws extend to other sectors, entities, data and practices that are not directly under the scope of their regulations, and whether they as a result improve the overall Internet security commons. As seen in the legislation, many instances of virtualized environments are actually explicitly out of scope of the legislation, above all on-premise, private cloud and virtualized environments. Nevertheless, when speaking of standardization, an important aspect to consider is not only the legal scope and delimitation of legislation but also the incentives that legal acts create for various entities, also those not directly in-scope, to implement better information security controls and best practices. In this sense, the GDPR and FISMA both convey broader responsibilities to CSPs and other actors offering and managing virtualized computing environments. The advent of the GDPR and its broad PII data oriented scope implies that data controllers who wish to host PII in the cloud will have to consider a number of challenges and requirements that will have to be guaranteed by the CSP. These include but are not limited to retention requirements, breach notification, extra-territorial data hosting, privacy controls and metadata management (Tolsma 2020). Effectively, in order to continue attracting clientele, CSPs must guarantee GDPR requirements, at least to a certain extent, otherwise they risk losing clients that are required to comply with the legislation. This is also visible with FISMA, particularly in case of the FedRAMP program. Once FedRAMP authorized, an organization offering cloud services is listed in the FedRAMP marketplace (see https://marketplace.fedramp.gov). Its listing and authorization imply that the service provider can compete for government contracts issued by all US federal agencies and institutions, a market that is otherwise inaccessible if not compliant. Considering that the US government is the largest employer in the US and also a hefty spender, many CSPs and other service providers will not want to miss the opportunity of competing for these government contracts and will therefore seek to improve the security posture of their environments and products as a result. This inadvertently creates more and better exposure for CSPs both as potential customers of other government institutions, as well as for private sector clients.

5.3 Jurisdiction

While laws are usually written for use and applicability to a specific jurisdiction, the wording and contents sometimes result in jurisdictional particularities. As HIPAA and FISMA are federal laws, they apply uniformly to all territorial jurisdictions that form the US, however certain provisions of HIPAA crucially allow for the superseding of state law in certain cases. Specifically, the law states that "if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation", the stronger State regulations will supersede the federal regulations (HIPAA 1996, Pub. L. 104-191, §264). With the recent introduction of the California Consumer Privacy Act (CCPA) in 2020, which is widely seen as the most stringent piece of data privacy legislation introduced anywhere in the US to date, this HIPAA clause is very significant as it allows for an unhindered development of more stringent provisions on a state level. Similar flexibility is given to EU member states by the NIS directive, as the resultant national legislation can be strengthened or adjusted at any point in time by the respective national legislators, a flexibility not awarded by the GDPR. The GDPR however, during its introduction also garnered considerable attention due to Article 3, which states that the territorial scope of the legislation applies also to foreign entities that are processing data of EU citizens, even if these are not based or have a presence within EU territory (Regulation 2016/679/EU, p. 32-33). Nevertheless, in keeping with the research question and aims of this paper, while far reaching jurisdictional scopes are good for security and privacy control standardization, the extraterritorial scope of the GDPR does not necessarily add any value to DDoS protection of entities within the Netherlands itself. For this reason, all four legislative documents can be considered equivalent in their jurisdictional prudence.

5.4 Other Considerations

Further to the above, a number of relevant aspects were explicitly not discussed or placed out of scope of this research paper. Although mentioned only briefly, enforceability, auditability and compliance with legislation is often a vague process. Security compliance is usually done by both government assigned auditors, as well as private sector compliance organizations. In this regard it is important to mention that compliance coverage reports can vary significantly in terms of both depth and scope, depending on which vendor covers the engagement (Yimam and Fernandez 2016, p. 6). Enforceability of the in-scope legislation was not discussed in depth due to the difficulty in accurately gauging the extent to which legislation is actually adhered to and what kind of exemptions, exceptions and rigidities are allowed within any given scope. While this is an important aspect to consider, it is nonetheless out of scope of the stated research question, as the intended purpose of the research was to determine the extent to which the two cases require the implementation of resistance and resilience strategies that mitigate DDoS attacks. A study into the extent of implementation of the identified variables or a comparative study comparing different auditability mechanisms (i.e. period compliance reviews, complaints-based audits, etc.) would thus certainly be an interesting direction for future research but is out of scope of this paper. Likewise, certain qualitative specifics were omitted due to the methodological and data collection design of this paper. To offer a concrete example, while both the GDPR and HIPAA require security breach reporting, therefore complying with this stated control, the requirements are significantly different for each law. Namely, while HIPAA requires a breach to be reported to the relevant authority within 60 days of having been detected, the GDPR demands the same requirement to be fulfilled in mere 72 hours after the initial breach was detected (45 CFR §164.408, 2013; Regulation 2016/679/EU, p. 52). While an in-depth study of the implications of this discrepancy is out of scope of this paper, it certainly presents an interesting possibility for future academic and research endeavours.

A further point of critique of the chosen research design was already briefly mentioned in chapter one and relates to the theoretical propositions of deterrence theory itself. Namely, the operationalization and theoretical postulation of what constitutes or influences gain value, gain probability, loss value or loss probability, is subjective and preconditioned on the rationalization of the attacker. In this sense, this study was not able to control the inherent weakness of the theory of deterrence in reconciling with the overreliance on rational behaviour assumptions as identified by the theory’s critics (Brantly 2018, p.33; Benediek and Metzger 2015, p. 556). As the purpose of this thesis was not to analyse criminal behaviour, but rather to assess a specific deterrence technique within a specific context, this issue did not have a significant influence on the results. Nevertheless, it does limit the generalizability of the results to a certain extent, namely by making them context specific. To offer an example, if the goal of an attacker is twofold, to first launch a DDoS attack to weaken defences and subsequently try to gain illegal access to a system via brute force or another secondary means, such a complex attack scenario would create a cost-benefit calculous that would not necessarily work with the criminological conceptualizations that were presented in this paper. While the identified controls would still impede the attacker from gaining value from the DDoS attack vector, they would not necessarily influence the attacker in the desired way so as to deter and prevent him or her from ultimately compromising the target system. While the overt reliance on rational assumptions is certainly a weakness within the theory of deterrence, the complex nature of the cybersecurity field implies that full-proof assumptions are very difficult, if not impossible. Context, particularly in a field characterized by low effort, high impact events, is thus of particular importance and should not be neglected, as previously stated.

6.0 CONCLUSION:

This thesis has aimed to establish the extent to which Dutch and American legislation obliges entities using or hosting virtualized computing environments to implement resistance and resilience strategies that mitigate the DDoS enabling design aspects of the Internet. Building upon the Internet design flaws identified by Mirkovic and Reiher (2004) and utilizing a comparative case study design, four key pieces of legislation from the two countries were analysed using a set of operationalized indicators based on DDoS deterrence by denial strategies (see 4.5 results table).

As an analysis of all legislation, including case law, precedents, legal interpretations and other guiding decisions, etc. was outside of the scope and limitations of this paper, the paper instead focused on crucial pieces of legislation within the two case countries, which were chosen due to their similar characteristics yet significantly different outcomes in terms of DDoS related cybercrime.

The analysis of the legislation and subsequent results revealed that American information security legislation more comprehensively covers and compels organizations to defend against DDoS attacks. While FISMA's 'commensurate approach', which tailors the information security policies and procedures to the needs of the particular government agency, might seem lax and distributed when compared to other legislation such as HIPAA or the GDPR, it importantly allows for a more targeted and data neutral application of controls. Acknowledging the fact that the federal government collects, processes, stores and ultimately protects an incredible variation of data of various kinds of sensitivity, the legislation approaches information security in a more comprehensive way than other equivalents by demanding high yet flexible standards from agencies with regards to information security guarantees, regardless of the data form, content, syntax or other specification.

Nevertheless, the legislative practices to guarantee information security in cloud and virtualization based environments and systems in both countries proved to be fragmented and limited in scope, often covering only a patchwork of various entities, systems, data and target groups. Various exceptions, technological complexity, and emphasis on business processes and subjects' rights, as opposed to information security technicalities, implies that the legislation more often than not only indirectly or very broadly targets the creation of resistance and resilience strengthening controls unitarily across the Internet. This implies that determining the extent of applicability of such controls is often left up to the managers and administrators of such environments, relying largely on industry best practices to guide organizations in their information security efforts. While this does not necessarily mean that such a regulatory approach is ineffective, it does imply that potential stragglers who neglect their information security duties within the Internet commons will continue to aggravate the security challenges for the rest of the community. DDoS attacks will thus also likely remain a viable and persistent threat in the future.

6.1 Avenues for Future Research:

While this study focused on cybercrime deterrence from the vantage point of the target, further information regarding the topic could be discerned with future avenues of research focusing on the perspective of the attacker. A shift in the level of analysis from the defender to the attacker by conducting empirical, including quantitative research would provide insights into whether the value assumptions of the two groups are aligned and what effect denial strategies have on the attacker. Furthermore, an analysis of a broader spectrum and depth of information security laws, specifically in terms of auditability and compliance mechanisms, might shed some further light on the tangible effects that regulation based information security standard making creates, as well as how it specifically affects certain types of organizations. Furthermore, as a final recommendation, in line with this paper's research goals of focusing on the mitigation of the Internet's DDoS enabling design aspects, this paper did not include every conceivable administrative, physical and technical control that could have a deterring effect on cybercriminals in a more general sense. Future research should endeavour to also conduct research within a broader scope of other technical and organizational deterrence aspects related to DDoS attacks more generally.

7.0 BIBLIOGRAPHY:

7.1 Works Cited:

Abhishta, A., Junger, M., Joosten, R., Nieuwenhuis, L. J. M. (2019). Victim Routine Influences the Number of DDoS Attacks: Evidence from Dutch Educational Network. *IEEE Security and Privacy Workshop (SPW)*: 242-247.

Ahmed, E., Ahmed, A., Yaqoob, I., Shuja, J., Gani, A., Imran, M., Shoaib, M. (2017). Bring Computation Closer toward the User Network: Is Edge Computing the Solution? *IEEE Communications Magazine*.

Akers, R. L. (1990). Rational Choice, Deterrence, and Social Learning Theory in Criminiology. The Path Not Taken. *The Journal of Criminal Law & Criminiology 81*(5): 653-676.

Alahmad, Y., Agarwal, A., Daradkeh, T. (2018). High Availability Management for Applications Services in the Cloud Container-Based Platform. *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*: 1-8.

Alomari, E., Gupta, B. B., Karuppayah, S., Alfaris, R., Manickam, S. (2012). Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *International Journal of Computer Applications 49*(7): 24-32.

Health Information Technology for Economic and Clinical Health Act of 2009, Public Law 111-5, 123 Stat. 226-279. Available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

Benediek, A. and Metzger, T. (2015). Deterrence theory in the cyber-century: Lessons from a state-of-the-art literature review. *2015 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik*: 553-570.

Blumenthal, M. S., and Clark, D. D. (2001). Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World. *ACM Transactions on Internet Technology 1*(1): 70-109.

Boerman, N., Henneke, M., Moura, G., Schaapman, G., de Weerdt, O. (2018). *The impact of DDoS attacks on Dutch enterprises*. Ede, Netherlands: Stichting Nationale Beheersorganisatie Internet Providers. Available at https://www.nbip.nl/wp-content/uploads/2018/11/NBIP-SIDN-DDoS-impact-report.pdf.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal 9(2):* 27-40.

Bowen, R., Ridruejo, D. L., Liska, A. (2002). *Apache Administrator's Handbook*. Carmel, Indiana: Sams Publshing.

Brantly, A. F. (2018). The Cyber Deterrence Problem. *2018 10th International Conference on Cyber Conflict*: 31-54.

Choras, M., Kozik, R., Flizikowski, A., Holubowicz, W., Renk, R. (2016). Cyber Threats Impacting Critical Infrastructures. In R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures* (pp. 139–161). Cham, Switzerland: Springer.

Cloudscene. (2021). Data Centers in Europe. Retrieved January 16, 2021, from https://cloudscene.com/datacenters-in-europe

Cooper, J. R. (2012). A New Framework for Cyber Deterrence. In Reveron, D. S. (Ed.), *Cyberspace and national security: threats, opportunities, and power in a virtual world* (pp. 105-120). Washington, D.C.: Georgetown University Press.

Cole, M. D., and Schmitz-Berndt, S. (2019). The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape. *University of Luxembourg Law Working Paper 2019*(017): 1-20.

Cole, E. (2009). *Network Security Bible, 2nd Edition*. Indianapolis, Indiana: Wiley Publishing.

Commission Implementing Regulation 2018/151. *Laying down rules for application of Directive (EU) 2016/1148 of 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*. European Commission. http://data.europa.eu/eli/reg_impl/2018/151/oj

Cybersecurity and Infrastructure Security Agency (2017). *US-CERT Federal Incident Notification Guidelines.* Arlington, Virginia: US Department of Homeland Security. Available at https://us-cert.cisa.gov/incident-notification-guidelines.

Cybersecurity and Infrastructure Security Agency (2018). *Cloud Security Guidance.* Arlington, Virginia: US Department of Homeland Security. Available at https://us-cert.cisa.gov/sites/default/files/publications/Cloud_Security_Guidance-.gov_Cloud_Security_Baseline.pdf.

DeCusatis, C., Liengtiraphan, P., Sager, A., Pinelli, M. (2016). Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. *2016 IEEE International Conference on Smart Cloud*: 5-10.

Dean, J. (2015). *The rise of cloud computing systems*. Lecture presented at SOSP History Day 2015 (SOSP '15), Article 12. New York, USA: 1-40. Available at https://dl.acm.org/doi/10.1145/2830903.2830913.

Denning, P. J. (1989). The ARPANET After Twenty Years. *American Scientist 77*(1): 530-535.

Directive 2016/1148. *Directive concerning measures for a high common level of security of network and information systems across the Union*. European Parliament, Council of the European Union. http://data.europa.eu/eli/dir/2016/1148/oj

Doerr, C., Gavrila, R., Kuipers, F., Trimintzios, P. (2012). *Good Practices in Resilient Internet Connection.* European Network and Information Security Agency (ENISA).

European Commission. (2012). Communication from The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing The Potential Of Cloud Computing In Europe. *COM 2012*(529): 1-16.

European Networks and Information Security Agency

European Union. (2020). Regulations, Directives and other acts. Retrieved January 10, 2021, from https://europa.eu/european-union/law/legal-acts_en.

Feng, W. C. (2003). The Case for TCP/IP Puzzels. *SIGCOMM Computer Communications Review 33*(4): 322-327.

Federal Information Security Management Act of 2014, 44 USC §§3551-3558. Available at https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

Govindan, R., Minei, I., Kallahalla, M., Koley, B., Vahdat, A. (2016). Evolve or Die: High-Availability Design Principles Drawn from Googles Network Infrastructure. *SIGCOMM '16: Proceedings of the 2016 ACM SIGCOMM Conference*: 58–72.

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 110 Stat. 1936-2102. Available at https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

U.S. Department of Health and Human Services. (2017). Enforcement Process. Retrieved January 10, 2021, from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

HIPAA Administrative Simplification, 45 CFR, §160-164 (2013). Available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

Houle, K. J., Weaver, G. M., Long, N., Thomas, R. (2001). *Trends in Denial of Service Attack Technology*. Pittsburgh, PA: CERT Coordination Center.

Hoque, N., Bhattacharyya, D. K., Kalita, J. K. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials* 17(4): 2242-2270.

Hussain, S. A., Fatima, M., Saeed, A., Razaa, I., Shahzadc, R. K. (2017). Multilevel classification of security concerns in cloud computing. *Applied Computing and Informatics Volume 13, Issue*: 57-65.

Jabbour, K. T., and Ratazzi, E. P. (2012). Does the United States Need a New Model for Cyber Deterrence? In Lowther, A. B. (Ed.), *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century* (pp. 33-45). New York, NY: Palgrave Macmillan.

Jahanbanifar, A., Khendek, F., Toeroe, M. (2014). Providing Hardware Redundancy for Highly Available Services in Virtualized Environments. *2014 Eighth International Conference on Software Security and Reliability (SERE)*: 40-47.

Joint Task Force Transformation Initiative Interagency Working Group (2014). *NIST Special Publication (SP) 800-53, Rev. 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-53r4

Kennedy, K. C. (1983). A Critical Appraisal of Criminal Deterrence Theory. *Digital Commons Law Review 88*(1): 1-13. Available at https://digitalcommons.law.msu.edu/facpubs/42/.

Knopf, J. W. (2010). The Fourth Wave in Deterrence Research. *Contemporary Security Policy 31*(1): 1-33.

Lopes, I. M., Guarda, T., Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. *14th Iberian Conference on Information Systems and Technologies (CISTI):* 1-6.

Mackieson, P., Shlonsky, A., & Connolly, M. (2018). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work*: 1-16.

(a) McKeay, M., Fakhreddine, A., Ragan, S., LaSeur, L. (2019). State of the Internet / Security. *A Year in Review 5*(6): 1-25. Available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-a-year-in-review-report-2019.pdf.

(b) McKeay, M., Fakhreddine, A., Ragan, S. (2019). DDoS and Application Attacks. *State of the Internet / Security 5*(1): 1-24. Available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf.

Ministerie van Economische Zaken en Klimaat – EZK (2018). *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners*. Den Haag, Nederland: Ministerie van Economische Zaken en Klimaat.

Mirkovic, J. and Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communications Review 34*(2): 39-54.

Mirkovic, J. and Reiher, P. (2008). Building accountability into the future Internet. *2008 4th Workshop on Secure Network Protocols*: 45-51.

Miura-Ko, R. A., Yolken, B., Mitchell, J., Bambos, N. (2008). Security Decision-Making Among Interdependent Organizations. *2008 21st IEEE Computer Security Foundations Symposium*: 66-80.

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide*. NIST Special Publication 800-61r2. Washington D.C.: NIST Research Library. http://dx.doi.org/10.6028/NIST.SP.800-61r2

National Institute of Standards and Technology. (2014). *Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*. NIST Special Publication 1108r3. Washington, D.C.: NIST Research Library. https://doi.org/10.6028/NIST.SP.1108r3

Nationaal Cyber Security Centrum. (2012). *Whitepaper NCSC Cloudcomputing & Security*. Den Haag, Netherlands: Ministerie van Justitie en Veiligheid. Available at https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cloudcomputing

Nieles, M., Dempsey, K., Pillitteri, V. Y. (2017). *An Introduction to Information Security*. NIST Special Publication 800-12r1. Washington, D.C.: NIST Research Library. https://doi.org/10.6028/NIST.SP.800-12r1

Office for Civil Rights. (2013). Summary of the HIPAA Security Rule. Retrieved January 10, 2021, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Office of Management and Budget (OMB). (2019). *Federal Information Security Modernization Act of 2014: Annual Report to Congress*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf

Oracle Corporation. (2014). 1.2 Reasons to Use Virtualization. Retrieved January 10, 2021, from https://docs.oracle.com/cd/E35328_01/E35332/html/vmusg-virtualization-reasons.html

Overvest, B. and Straathof, B. (2015). What drives cybercrime? Empirical evidence from DDoS attacks. The Hague, Netherlands: CPB Netherlands Bureau for Economic Policy Analysis.

Pearson, S., Tountopoulos, V., Catteddu, D., Südholt, M., Molva, R., Reich, C., Fischer-Hübner, S., Millard, C., Lotz, V., Jaatun, M. G., Leenes, R., Rong, C., Lopez, J. (2012). Accountability for cloud and other future Internet services. *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*: 629-632.

Pfleeger, C. P., Pfleeger, S. L., Margulies, J. (2015). *Security in Computing, 5th Edition*. Noida, India: Pearson.

Radware. (2017). History of DDoS Attacks. Retrieved January 10, 2021, from https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/

Regulation 2016/679. *Regulation on 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).* European Parliament, Council of the European Union. http://data.europa.eu/eli/reg/2016/679/oj

Rosenblum, M. (2004). The Reincarnation of Virtual Machines. *Queue 2*(5): 35-40.

Ross, R., Katzke, S., and Toth, P. (2005). The new FISMA standards and guidelines changing the dynamic of information security for the federal government. *MILCOM 2005 - 2005 IEEE Military Communications Conference 2(1)*: 864-870.

SANS Institute. (2020). Information Security Resources. Retrieved January 10, 2021, from https://www.sans.org/information-security/

Seeley, D. (1989). A Tour of the Worm. *University of Utah Computer Science Technical Report 89*(9): 1-15. Available at https://collections.lib.utah.edu/ark:/87278/s6st86z0.

Sigholm, J. (2016). Non-State Actors in Cyberspace Operations. *Journal of Military Studies 4*(1): 1-37.

Siponen, M. and Vance, A. (2010). New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly 34*(3): 487-502.

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy and future directions. *Computer Communications 107*(1): 30-48.

Spafford, E. H. (1988). The Internet Worm Program: An Analysis. *Purdue University Department of Computer Science Technical Reports 702*(1): 1-40.

Stamatelatos, N. (2006). A Measurement Study of BGP Blackhole Routing Performance. [Master's dissertation, Naval Postgraduate School]. NPS Archive: Calhoun. https://apps.dtic.mil/sti/pdfs/ADA457366.pdf

Subramanian, N., Jayaraj, A. (2018). Recent security challenges in cloud computing. *Computers and Electrical Engineering 71*(1): 28-42.

Syam, P. (2014). What is the Difference Between Common Law and Civil Law? Retrieved December 27, 2020, from https://onlinelaw.wustl.edu/blog/common-law-vs-civil-law/

Uptime Institute. (2021). Uptime Institute Issued Awards. Retrieved January 16, 2021, from https://uptimeinstitute.com/uptime-institute-awards/list

Urquhart, L., Lodge, T., Crabtree, A. (2019). Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology 27*(1): 1-27.

Usa.gov. (2020). How Laws Are Made. Retrieved January 10, 2021, from https://www.usa.gov/how-laws-are-made.

Van Roekel, S. (2011). *OMB Memorandum December 8, 2011: Security Authorization of Information Systems in Cloud Computing Environments*. Retrieved from: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

Verma, A., Arif, M., Husain, M. S. (2018). Analysis of DDOS Attack Detection and Prevention in Cloud Environments: A Review. *International Journal of Advanced Research in Computer Science 9*(2): 107-113.

Voss, G. W., and Houser, K. A. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal 56*(2): 287-344.

Tchernykh, A., Schwiegelsohn, U., Talbi, E., and Babenko, M. (2016). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of computational science 36*(1): 1-9.

Tolsma, A. (2020). GDPR and the impact on cloud computing. Retrieved January 10, 2021, from https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html

Trujillo, C. (2014). The Limits of Cyberspace Deterrence. *Joint Force Quarterly 75*(1): 43-52.

Wallace, L., Lin, H., Cefaratti, M. A. (2011). Information Security and Sarbanes-Oxley Compliance: An Exploratory Study. *Journal of Information Systems 25*(1): 185-211.

Wang, Q., Dunlap, T., Cho, Y., Qu, G. (2017). DoS Attacks and Countermeasures on Network Devices. *2017 26th Wireless and Optical Communication Conference* (WOCC): 1-6.

Wang, A., Mohaisen, A., Chang, W., and Chen, S. (2018). Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis. *IEEE/ACM Transactions on Networking*: 1-13.

Wet beveiliging netwerk- en informatiesystemen, *Stb.* 2018, 387. Available at https://zoek.officielebekendmakingen.nl/stb-2018-387.html.

De Weerdt, O., Schaapman, G., Pegtel, W., Zondervan, S. (2020). *DDoS data report 2019*. Ede, Netherlands: Stichting Nationale Beheersorganisatie Internet Providers. Available at https://www.nbip.nl/wp-content/uploads/2020/06/NBIP-DDoS-data-report-2019.pdf.

White, D. M. (2010). The Federal Information Security Management Act of 2002: A Potemkin Village. Fordham Law Review 79(1): 369-405.

Wilner, A.S. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies 43*(2): 245-280.

Williams, S. (2020). CCPA Tipping the Scales: Balancing Individual Privacy with Corporate Innovation for a Comprehensive Federal Data Protection Law. *Indiana Law Review 53*(217): 217-243.

World Bank. (2021). Individuals using the Internet (% of population) - Netherlands, United States. Retrieved January 16, 2021, from https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=NL-US

Yimam, D. and Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications 7*(5): 1-12.

Yin, R. K. (2009). *Case Study Research Design and Methods Fourth Edition*. Thousand Oaks, California: Sage Publications, Inc.

7.2 Works Consulted:

Fultz, N., Grossklags, J. (2009). Blue versus Red: Towards a Model of Distributed Security Attacks, In Financial Cryptography and Data Security. *Lecture Notes in Computer Science 5628*(1): 167-183.

Hashmi, M. J., Saxena, M., Saini, R. (2012). Classification of DDos Attacks and their Defence Techniques using Intrusion Prevention System. *International Journal of Computer Science & Communication Networks 2*(5): 607-614.

Joshi, B., Vijayan, A. S., Joshi, B. K. (2012). Securing Cloud Computing Environment Against DDoS Attacks. *2012 International Conference on Computer Communication and Informatics*: 1-5.

Karami, M., Park, Y., McCoy, D. (2016). Stress testing the booters: Understanding and undermining the business of DDoS services. *Proceedings of the 25th International Conference on World Wide Web*: 1033–1043.

Liu, P., Zang, W., Yu, M. (2005). Incentive-based modelling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security 8*(1): 78-118.

Mansfield-Devine, S. (2014). The evolution of DDoS. *Computer Fraud and Security 2014*(10): 15-20.

Mousavi, S. M., and St-Hilaire, M. Early Detection of DDoS Attacks Against SDN Controllers. *2015 International Conference on Computing, Networking and Communications*: 77-81.

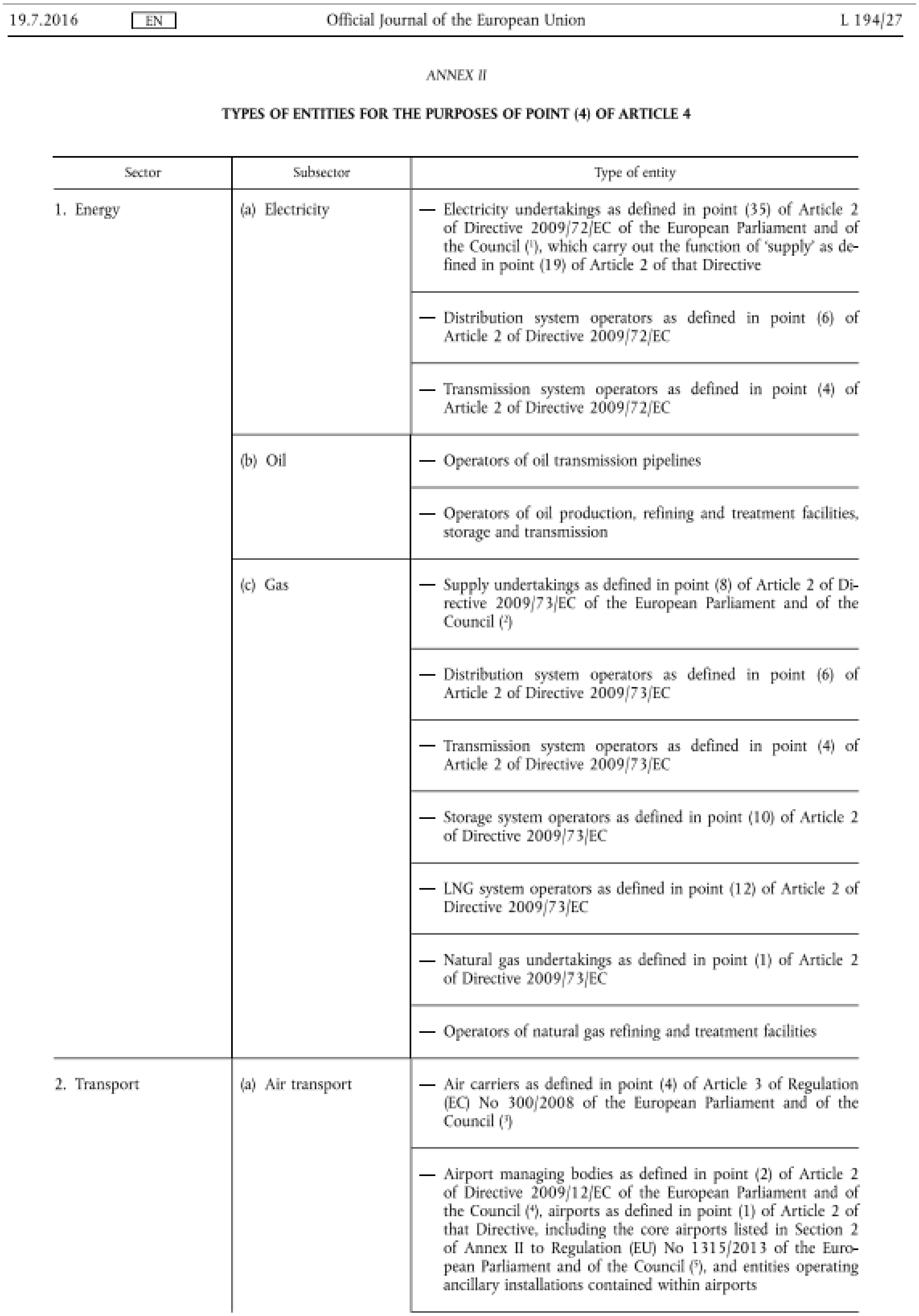
Zarger, S. T., Joshi, J., Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials 15*(4): 2046-2069.

Appendix 1:

Entity:	Responsible for:
Federal agencies	• Overall cyber security posture of the respective agency. • "Agencies are ultimately responsible for allocating the necessary people, processes, and technology to protect Federal data."
Office of Management and Budget (OMB)	• Oversight of information security and privacy practices of federal agencies and other in-scope institutions; • Development and implementation of policies and guidelines.
Office of Information and Regulatory Affairs	• Providing assistance on privacy matters; • Oversight and implementation of privacy policy of federal agencies.
National Institute of Standards and Technology (NIST)	• Developing and maintaining standards and guidelines for the effective protection of national information and information systems.
National Security Council (NSC)	• Implementation of an administration's cyber security priorities.
Department of Homeland Security (DHS)	• Regulatory authority; • Providing technical and operational guidance and assistance; • Coordination of government-wide cyber security efforts.
General Services Administration (GSA)	• Providing management and administrative support; • Hosting the Federal Risk and Authorization Management Program (FedRAMP).
Federal Bureau of Investigation (FBI)	• Investigating cyber security intrusions, incidents and attacks.
The intelligence community	• Obtaining and analysing information on cyber threats and malicious actors.

(Office of Management and Budget 2019, p.6-7; FISMA 2014, 44 USC §3553).

Appendix 2:

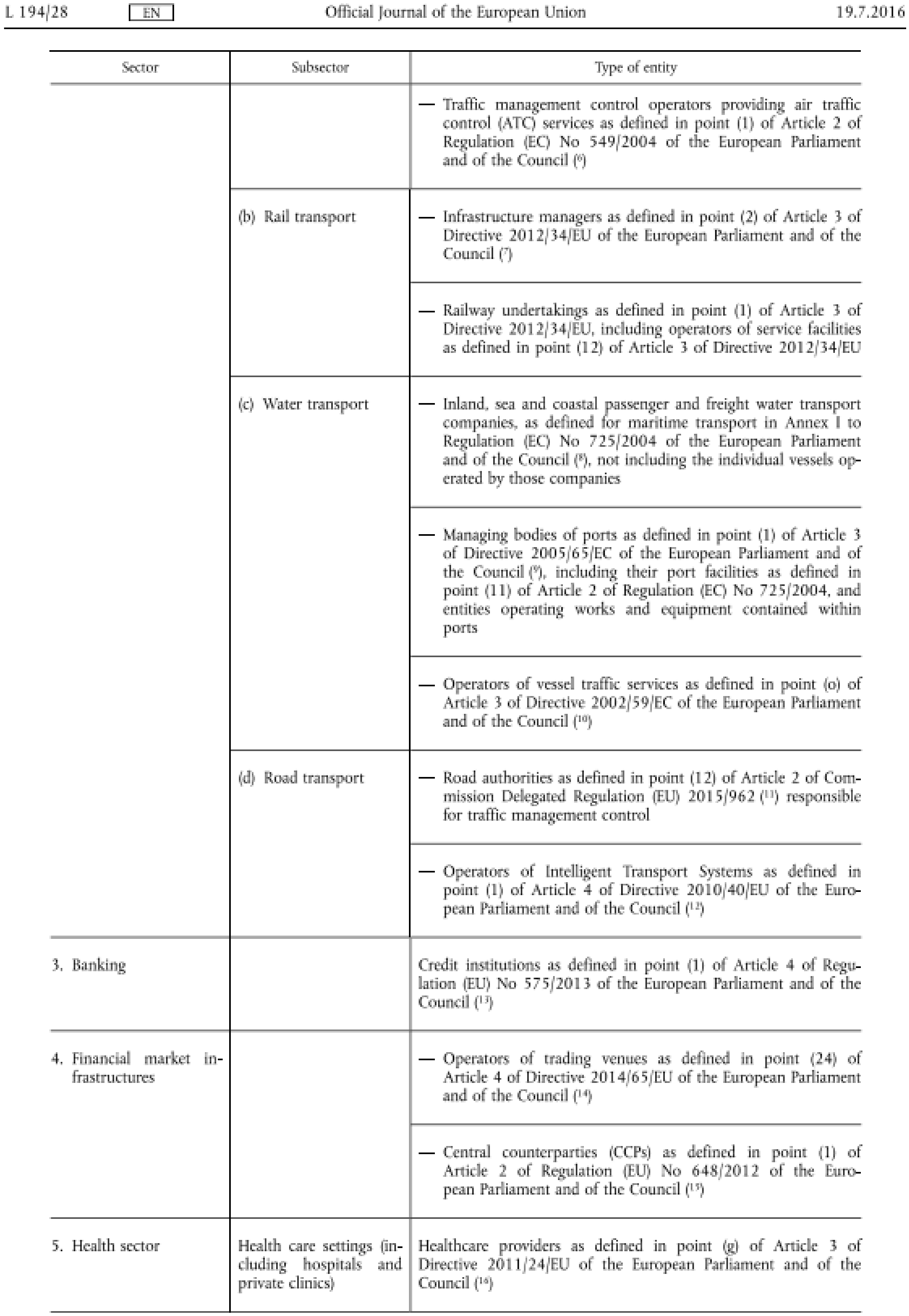


19.7.2016 EN Official Journal of the European Union L 194/27

ANNEX II

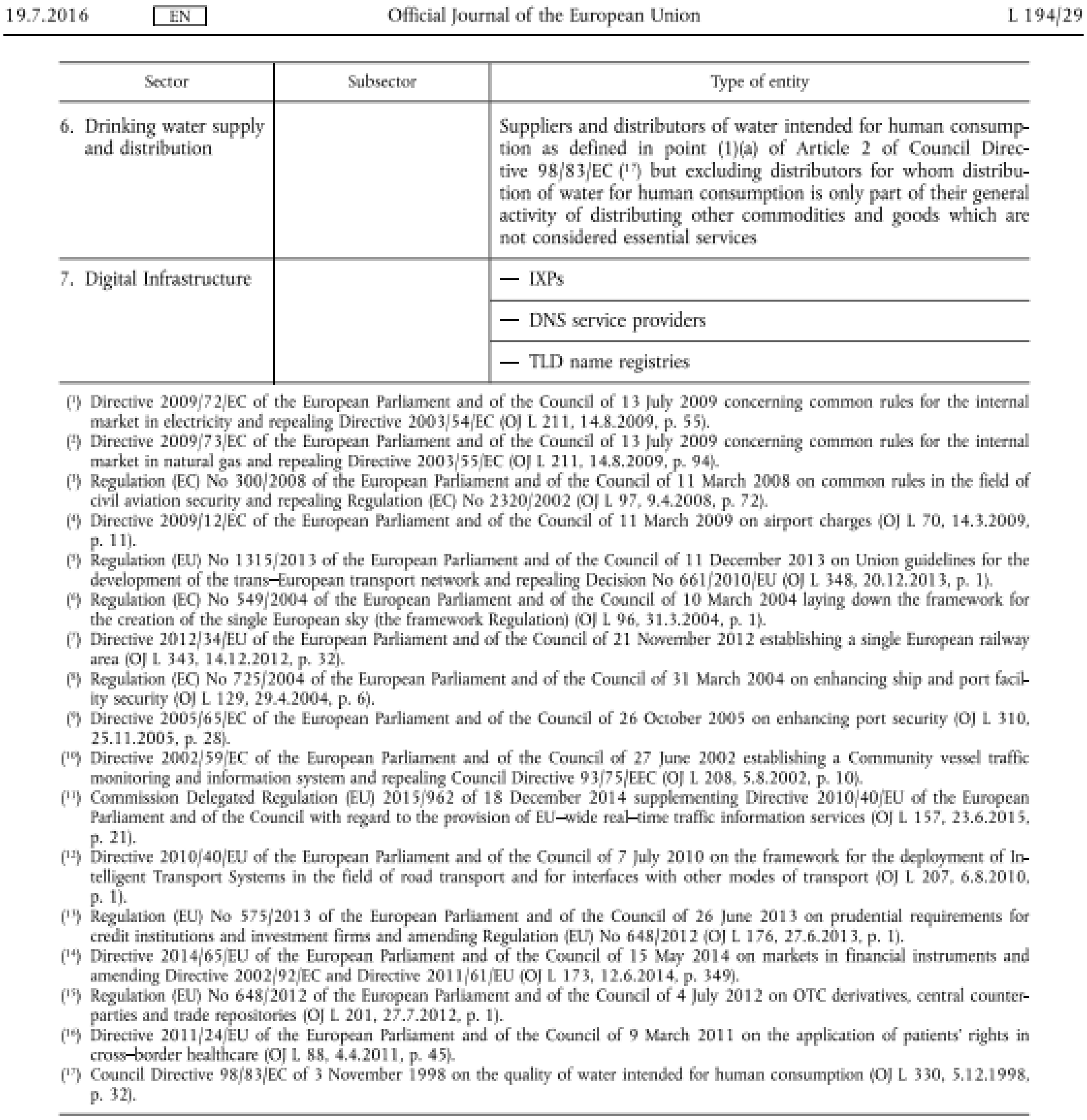
TYPES OF ENTITIES FOR THE PURPOSES OF POINT (4) OF ARTICLE 4

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council [1], which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive
		— Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC
		— Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC
	(b) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
	(c) Gas	— Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council [2]
		— Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC
		— LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
2. Transport	(a) Air transport	— Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council [3]
		— Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council [4], airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council [5], and entities operating ancillary installations contained within airports



L 194/28 EN Official Journal of the European Union 19.7.2016

Sector	Subsector	Type of entity
		— Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council (6)
	(b) Rail transport	— Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council (7)
		— Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water transport	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council (8), not including the individual vessels operated by those companies
		— Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council (9), including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council (10)
	(d) Road transport	— Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 (11) responsible for traffic management control
		— Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council (12)
3. Banking		Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council (13)
4. Financial market infrastructures		— Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council (14)
		— Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council (15)
5. Health sector	Health care settings (including hospitals and private clinics)	Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council (16)



19.7.2016 EN Official Journal of the European Union L 194/29

Sector	Subsector	Type of entity
6. Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC [17] but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services
7. Digital Infrastructure		— IXPs
		— DNS service providers
		— TLD name registries

[1] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (OJ L 211, 14.8.2009, p. 55).

[2] Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

[3] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

[4] Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

[5] Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans–European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

[6] Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).

[7] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).

[8] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

[9] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

[10] Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

[11] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21).

[12] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

[13] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

[14] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

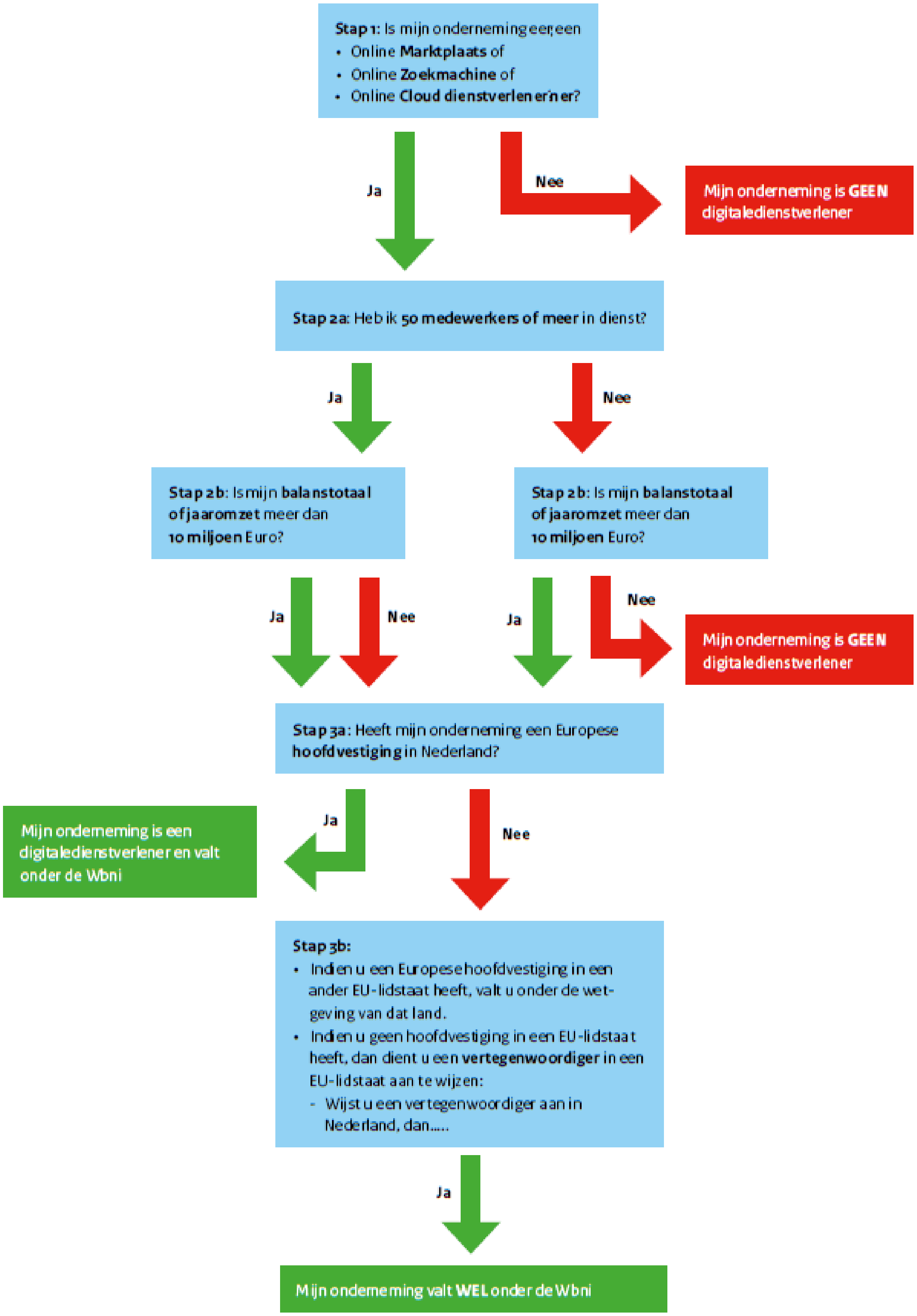
[15] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

[16] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45).

[17] Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

(Directive 2016/1148/EU, p.27-29)

Appendix 3:


Stap 1: Is mijn onderneming een, een
• Online Marktplaats of
• Online Zoekmachine of
• Online Cloud dienstverlener?
Ja
Nee
Mijn onderneming is GEEN digitaledienstverlener
Stap 2a: Heb ik 50 medewerkers of meer in dienst?
Ja
Nee
Stap 2b: Is mijn balanstotaal of jaaromzet meer dan 10 miljoen Euro?
Stap 2b: Is mijn balanstotaal of jaaromzet meer dan 10 miljoen Euro?
Ja
Nee
Ja
Nee
Mijn onderneming is GEEN digitaledienstverlener
Stap 3a: Heeft mijn onderneming een Europese hoofdvestiging in Nederland?
Ja
Nee
Mijn onderneming is een digitaledienstverlener en valt onder de Wbni
Stap 3b:
• Indien u een Europese hoofdvestiging in een ander EU-lidstaat heeft, valt u onder de wetgeving van dat land.
• Indien u geen hoofdvestiging in een EU-lidstaat heeft, dan dient u een vertegenwoordiger in een EU-lidstaat aan te wijzen:
- Wijst u een vertegenwoordiger aan in Nederland, dan.....
Ja
Mijn onderneming valt WEL onder de Wbni

(Ministerie van EZK 2018, p.5)