UNIVERSITY OF GDAŃSK - FACULTY OF ECONOMICS

Marc Wilczek

Field of science: Social Sciences
Scientific discipline: Economics and Finance

Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases

PhD dissertation prepared under supervision of
dr hab. Monika Bąk, prof. UG

September 16, 2024

STRESZCZENIE

Podejmowanie decyzji w warunkach ograniczeń: perspektywa ekonomii behawioralnej na heurystyki i uprzedzenia związane z cyberprzestrzenią

Marc Wilczek

Wzrastająca liczba przestępstw cybernetycznych stanowi coraz większe zagrożenie dla organizacji na całym świecie. Incydenty związane z bezpieczeństwem cybernetycznym mogą prowadzić do poważnych strat finansowych i strategicznych, a systemowy charakter ryzyka cybernetycznego oznacza, że złe decyzje i incydenty w jednym obszarze mogą szybko się rozprzestrzeniać i wpływać na niepowiązane podmioty. Aby poradzić sobie z tym zagrożeniem, kluczowe jest przyjęcie holistycznego i interdyscyplinarnego podejścia, które obejmuje zarówno rozwiązania technologiczne, jak i uwzględnienie zachowań ludzkich.

Człowiek jako element bezpieczeństwa cybernetycznego często jest pomijany, ale jest on kluczowy dla skutecznej cyberodporności. Procesy podejmowania decyzji w tym kontekście są podatne na błędy w osądzie, co prowadzi do niewłaściwych ocen powodujących dalekosiężne konsekwencje. Błędy poznawcze i heurystyki odgrywają w tym kontekście istotną rolę, ale brakuje badań nad ich wpływem w dziedzinie bezpieczeństwa cybernetycznego, zwłaszcza jeśli chodzi o eksplorację zachowań i opinii ekspertów w tej dziedzinie.

W pracy podjęto kompleksową analizę istniejącej literatury dotyczącej błędów poznawczych i heurystyk w obszarze cyberbezpieczeństwa. Dodatkowo przeprowadzono wywiady z ekspertami, którzy posiadają dogłębną wiedzę w konkretnym obszarze. Głównym celem pracy jest zbadanie zakresu błędów poznawczych i ich wpływu na procesy decyzyjne dotyczące cyberbezpieczeństwa. Wyniki badań zostaną wykorzystane do opracowania praktycznych zaleceń, które mogą pomóc specjalistom i organizacjom zajmującym się cyberbezpieczeństwem złagodzić negatywny wpływ błędów poznawczych i heurystyk na podejmowanie decyzji dotyczących cyberbezpieczeństwa.

Przyczynią się zatem do rozwoju kompleksowego podejścia do cyberbezpieczeństwa, które kładzie nacisk szczególny nacisk na zrozumienie ludzkich zachowań. Rozumiejąc wpływ błędów poznawczych i heurystyk na podejmowanie decyzji dotyczących cyberbezpieczeństwa, specjaliści ds. cyberbezpieczeństwa mogą podejmować świadome i skuteczne decyzje, które ostatecznie prowadzą do lepszej wydajności i mniejszego narażenia ich organizacji i całego otoczenia społecznego na zagrożenia cybernetyczne.

Słowa kluczowe: Cyber-ryzyko, cyberprzestępczość, podejmowanie decyzji, błędy poznawcze, heurystyki.

ABSTRACT

Decision-Making under Constraints: A Behavioral Economics Perspective on Cyber-Related Heuristics and Biases

Marc Wilczek

The increasing prevalence of cybercrime is a growing concern for organizations worldwide. Cyber-security incidents can result in significant financial and strategic losses, and the systemic nature of cyber-risks means that poor decisions and incidents in one area can quickly spread and impact unrelated entities. To address this danger, it is crucial to adopt a holistic and interdisciplinary viewpoint that includes both technological measures and consideration of human behavior.

The human element of cyber-security is often overlooked, but it is crucial to establishing effective cyber-resilience. Decision-making processes in this context are susceptible to judgmental flaws, leading to suboptimal outcomes with far-reaching consequences. Cognitive biases and heuristics play a significant role in this context, but there is a lack of research on their impact in the field of cyber-security, especially when it comes to subject matter experts.

This thesis will encompass an extensive examination of the existing literature regarding cognitive biases and heuristics within the cyber-security domain. Moreover, it will involve conducting interviews with experts who possess profound knowledge in this field. The primary goal of this thesis is to delve into the extent of cognitive distortions and their influence on decision-making processes concerning cyber-security. The outcome of this study will be utilized to develop practical recommendations that can aid cyber professionals and organizations in mitigating the adverse effects brought about by cognitive biases and heuristics on decision-making in cyber-security. The overarching objective of this thesis is to contribute to the advancement of a more all-encompassing approach to cyber-security that prioritizes the understanding of human behavior. By comprehending the impact of cognitive biases and heuristics on cyber-security decision-making, cyber professionals will be empowered to make well-informed and effective decisions, ultimately leading to better outcomes, and reduced cyber-risk exposure for their organizations.

Keywords: Cyber-Risk, Cybercrime, Decision-Making, Cognitive Biases, Heuristics

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to Prof. Dr. Monika Bąk for her exceptional support, accessibility, and inspiring exchange of ideas. Her guidance and mentorship throughout this journey have been invaluable, and I could not have imagined better leadership for this research project. It was a great pleasure to collaborate with her.

I would also like to acknowledge Jens-Phillip Jung, Tim Wybitul, and Carsten Meywirth for generously sharing their time and insights during the background interviews. Their contributions significantly shaped the academic discourse of this thesis. A special thanks goes to Ralph Noll and his fantastic team at Deloitte, who not only made the data collection possible but also facilitated a background interview and supported the research project wholeheartedly.

Additionally, I would like to extend my thanks to Prof. Dr. Michal Suchanek, Prof. Dr. Lutz Hofmann, and Dr. Hugo Martins for being valuable sparring partners throughout this process.

LIST OF PUBLICATIONS

Wilczek, M. (2024). Exploring the Potential of Behavioral Economics in Cyber-Security: Development of a Conceptual Framework. *International Business and Global Economy (IBaGE)*. ISSN 2300-6102 (accepted: 04/2024)

Wilczek, M. (2022). The Importance of Security for the Crypto Industry. *Computer Fraud & Security*. 2022(10). https://doi.org/10.12968/S1361-3723(22)70596-9

Wilczek, M. (2021). IoT – die unterschätzte Gefahr für IT-Sicherheit. *Datenschutz und Datensicherheit*. 2021(45), 79–82. https://doi.org/10.1007/s11623-021-1394-5

Table of Contents

GLOSSARY

Advanced Persistent Threat (APT)

An APT is a stealthy threat actor, typically a nation state or state-sponsored group that has the means, resources, and capabilities to conduct some of the most sophisticated and complex cyber operations.

Al-Qaida

A loose, globally operating terrorist network of mostly Sunni Islamist organizations.

Application Programming Interface (API)

A programmable interface which facilitates communication between diverse applications.

Asia Pacific (APAC)

Depending on the context, the Asia-Pacific region varies in area but typically includes countries in East Asia, Southeast Asia, and Oceania.

Attack Vector

A specific path, method, or scenario utilized by a threat actor to accomplish the objective.

Attribution

The identification of the threat actor accountable for a specific series of actions.

Australian Cyber Security Centre (ACSC)

The Australian Government's cyber-security body.

Bank Run

A bank run happens when a bank is overwhelmed by clients trying to withdraw their funds in fear that the bank may default anytime soon. Unless interfered quickly, this can turn into a self-fulfilling prophecy and produce a domino effect. As more people withdraw cash, the situation escalates and the default risk increases, causing further withdrawals.

Blue Team

A group or unit that is typically responsible for defending an organization’s digital assets and infrastructure against cyber-attacks (see “red team”).

Big Game Hunting

A sophisticated cyber operation aimed at large-scale or organizations or high-profile entities (so called high-value targets) primarily with the intend to take down prestigious targets and/or pocket large amounts of money.

Big Tech

The collective of the largest IT companies in the world.

Brute Force Attack

A trial-and-error method by hackers, often automated at scale, whereby a wide range of username and password combinations are used to illegally gain access.

Central Intelligence Agency (CIA)

The foreign intelligence service of the United States.

Chinese Communist Party (CCP)

The founding and sole ruling party of the People’s Republic of China.

Command-and-Control (C&C) Server

A server is used to control a compromised system, allowing attackers to inject malicious code, steal data, and operate unnoticed as part of a botnet.

Content Delivery Network (CDN)

It enables the efficient delivery of web content by distributing it across multiple servers in different locations, reducing latency and improving performance.

Council on Foreign Relations (CFR)

An independent, nonpartisan membership organization, think tank, and publisher.

Critical Infrastructure

Assets, systems, and networks, whether physical or virtual, which are considered essential for society such as power grids, pipelines, communication networks, health care, railroads, and so on. Because of the consequences of a successful attack, critical infrastructure is considered a prime target for state-sponsored actors, terrorists, and hacktivists alike.

Cyberbullying

Insulting, threatening, embarrassing, or harassing anyone using digital channels including social media.

Cyber-Grooming

The targeted manipulation of minors and young adults via the internet. The goal is to lure the victim into a trap to commit sexually motivated crimes.

Cyber-Security

An umbrella term encompassing IT security but also other areas like protecting against cyber-threats, managing risk, and ensuring the overall security of digital and cyber-physical systems.

Cyberstalking

Also referred to as digital stalking or online stalking, cyberstalking refers to the stalking, tracing, and monitoring of a person with electronic means.

Cybersecurity and Infrastructure Security Agency (CISA)

The U.S. Government's cyber-security body, a division of the U.S. Department of Homeland Security.

DACH-Region (or D-A-CH region)

An acronym comprising Germany (D), Austria (A), and Switzerland (CH).

Dark Web

A clandestine subterranean network that enables individuals to communicate and exchange files with utmost anonymity and security. While accessible to any internet user through specific browsers, it poses a significant challenge to identify the individuals operating the sites, as they remain concealed from search engine results.

Deep Fakes

Media content that appears realistic but has been altered, generated, or manipulated through artificial intelligence.

Deep Web

All websites that are not searchable by conventional search engines and are predominantly employed for routine tasks.

Digital Natives

Although definitions may vary, for the purpose of this thesis the term refers to the cohort of so-called Generation Y (born post 1980) and Generation Z (Millennials), effectively those who grew up in the “digital age” and have been influenced by computers, mobile phones, the internet, and social media.

Digital Technology

An umbrella term encompassing various advanced and value-creating information and communication technology (ICT) that aid in the creation, storage, and management of data, ultimately contributing to the advancement and transformation of society.

Digitalization

The adoption, integration and usage of digital technology across business and society, fundamentally changing operating, business, and revenue models as well as human interaction with one another.

Distributed Denial of Service (DDoS)

Cyber-attacks which are maliciously flooding servers or network resources with bad traffic to the extent that the respective service collapses and become unavailable for legitimate usage.

Domain Name Server (DNS)

Fulfills a critical role in internet communication by translating domain names (URLs) into IP addresses, making it easier for users to access websites and online resources without having to remember complex IP addresses.

Dual War

With cyberspace turning into a joint warfighting domain, dual war describes the concept of a military conflict that is two dimensional, for example the combination of conventional warfare flanked by cyber-operations (see multi-domain conflict and/or hybrid warfare).

East Midlands Cyber Resilience Centre (EMCRC)

A Police-led partnership tasked with improving cyber-resilience across the UK's East Midlands.

European Union Agency for Network and Information Security (ENISA)

An EU cyber-security agency tasked with keeping Europe's society digitally secure.

Europol

The EU agency for law enforcement cooperation, tasked with combating organized crime, terrorism, and international crime.

False Flag Operations

A misleading maneuver to erroneously attribute an activity to a different party.

Federal Bureau of Investigation (FBI)

The domestic intelligence and principal federal law enforcement agency of the United States.

Federal Security Service (FSB)

The principal security agency of Russia and the main successor of KGB.

Fin7

A Russia-based criminal APT group, considered to be among the most successful in the world.

Five Eyes (FVEY)	An intelligence alliance encompassing Australia, Canada, New Zealand, the United Kingdom, and the United States.
Foreign Intelligence Service (SVR)	Russia’s foreign espionage and intelligence agency.
General Data Protection Regulation (GDPR)	A regulation on information privacy and data protection across the EU. Severe violations can incur fines of up to €20 million or 4% of annual revenue per breach, whichever is higher. For multiple breaches, fines can be cumulative, resulting in potentially very high penalties.
General Staff Intelligence Directorate (GRU)	Russia’s foreign military intelligence agency.
Hacktivist	An activist employing hacking skills for political or ideological reasons.
Hybrid Warfare	The fusion of various military and non-military tactics to blur the line between war and peace, using both conventional and unconventional methods.
Industrialization	A transformation process from a labor-intense economy to an industrial economy in which products are no longer made by hand but with the help of machines and factories.
Internal Revenue Service (IRS)	A U.S. agency responsible for the administration and enforcement of the country’s tax laws.
International Data Corporation (IDC)	A U.S. market intelligence firm.
Internet of Things (IoT)	The collective of internet-facing smart devices equipped with sensors to store and process data.

Interpol	The world’s largest organization coordinating cooperation and crime control across 195 member states.
IP address	An internet protocol address is a unique numerical identifier that is linked to a particular computer or network.
Islamic State (ISIS or IS)	A militant terrorist organization.
IT Security	Focused on securing specific IT systems and infrastructure within an organization.
Killnet	A pro-Russian hacktivist group.
Know Your Customer (KYC)	In specific sectors, a compulsory identification verification process to prevent money laundering.
Malware	Malicious software designed to harm or exploit computer systems, networks, and devices. It can take various forms, such as viruses, worms, Trojans, ransomware, spyware, adware, and rootkits.
Ministry of Intelligence and Security (MOIS)	The primary intelligence agency (otherwise known as VAJA and previously VEVAK) of the Islamic Republic of Iran.
Monero	A cryptocurrency that is distinguished by its stringent focus on safeguarding user anonymity and data protection
Multi-Domain Conflict	A military confrontation that encompasses multiple domains (sea, air, land, cyber, or space).
National Cyber Crime Unit (NCCU)	The cyber command of the United Kingdom’s National Crime Agency.
National Health Service (NHS)	An umbrella term for the publicly funded healthcare systems of the United Kingdom.

National Security Agency (NSA)

A United States intelligence agency, tasked with global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes.

National Institute of Standards and Technology (NIST)

A U.S. standard setting body and an agency of the United States Department of Commerce.

NIS Corporation Group

An EU format comprising Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA) to facilitate strategic cooperation between the Member States regarding the security of network and information systems.

Obfuscation

Tactics and tools used by threat actors to shield their identities, goals, techniques, and even their victims.

Personally Identifiable Information (PII)

Any data that could theoretically be used to identify a specific individual. Examples of this are names, tax identification numbers, account details or telephone numbers.

Phishing

Fraudulent e-mails, text messages, phone calls, or websites aim to deceive individuals into downloading malware and disclosing sensitive information.

Ransom DDoS (RDDoS or RDoS)

A method—sometimes part of a wide-ranging extortion campaign—in which bad actors threaten their victims to unleash DDoS attacks unless a ransom fee, typically in form of cryptocurrency, so that the transaction cannot be traced by law enforcement, is being paid.

Ransomware

A specific type of malware that makes data inaccessible until a ransom has been paid.

Red Team
A group of individuals tasked with simulating cyber-attacks and strategies to identify vulnerabilities within a system or organization (see “blue team”).

REvil
A Russia-based or Russian-speaking Ransomware-as-a-Service (RaaS) syndicate.

Run on the Banks
See “Bank run”.

Script Kiddies (or Skids)
An immature individual (typically a teenager) who engages in cybercrime, often by using 3rd party tools, with little consideration of the potentially harmful consequences.

STEM
An acronym referring to science, technology, engineering, and mathematics.

Stuxnet
A malware that has garnered significant attention due to its unique characteristics and implications. It was specifically developed to target industrial control systems, particularly those used in nuclear facilities.

Trojan
As it relates to computers, a malware that disguises itself as a genuine program or file to gain unauthorized access to a computer network.

Uniform Resource Locator (URL)
A standardized address used to locate resources on the internet.

Uptime
The reliance of a computer system (or any ICT component in that matter), measured in the quotient of availability. Uptime is the opposite of downtime.

Virtual Private Network (VPN)
An encrypted connection, protecting privacy, and unblocking restricted content. They are

especially useful to undermine surveillance or censorship.

World Economic Forum (WEF)

An organization bringing together political, business, cultural and other leaders of society to discuss global concerns, best known for their annual meeting held in Davos, Switzerland.

Worm

In the computer context, a malware that replicates itself and spreads across networks without requiring any user interaction.

CHAPTER 1
INTRODUCTION

1.1 Motivation

When it comes to gaining cyber-resilience, a lot of emphasis is typically put on the deployment of technology and the release of guidelines, policies, and processes. The spending on cyber-security has soared over the past years, with spending projected to climb from US$219 billion in 2023 to over US$300 billion by 2026 IDC (2023). Despite these large investments, cyber-threats keep proliferating, a phenomenon known as the "Cyber Paradox" (Bone, 2016; Nikkhah & Grover, 2022). Based on these findings, the efficacy of conventional cyber-security measures has come into question (Bone, 2016; Kianpour et al., 2021). Additionally, cyber-threats are instigating more and more *externalities.* Of 3,600 executives interviewed across 550 different organizations, 83% reported that they have already encountered more than one data breach (IBM/Ponemon Institute, 2022). As highlighted by Forrester Research, companies may be investing more in cyber defense, but often not in the most effective areas (Blackborow & Christakis, 2019). A pivotal aspect of turning the tide entails recognizing the significance of human behavior during the design, construction, and utilization of cyber-security technology (Pfleeger & Caputo, 2012). Regardless of the level of perfection in an organization's cyber-security posture, its effectiveness will invariably largely rely on human behavior (Maalem Lahcen et al., 2020; Rodriguez-Priego & Bavel, 2023; Stanton et al., 2004).

According to historical accounts, Sir Isaac Newton purportedly stated, *"I can calculate the movement of stars but not the madness of men."* Indeed, the susceptibility to humans cannot be overstated, they are widely regarded as a significant contributor to cyber-security incidents (Alsharida et al., 2023; Frank, 2020; Kostyuk & Wayne, 2020; Kovačević et al., 2020; Rosoff et al., 2013) and often referred to as the "weakest link in the chain" (e.g., Alnifie & Kim, 2023; Bone, 2016; Hewitt & White, 2022; Singh & Bakar, 2019; Siponen, 2000; White, 2015). Research suggests that approximately 25% of all cyber-security incidents are caused by human error (Waldrop, 2016). When it comes to data breaches, which is one specific kind of a cyber-security incident and arguably one of the most severe with a leakage of sensitive data being the result, researchers from Stanford University have concluded that even 88% of all data breaches can be back traced to human error (Hancock, 2022). The primary factor contributing to this trend are judgmental flaws in cyber-risk assessment and insufficient implementation of precautions (Alnifie & Kim, 2023). The results of such human error can be incredibly expensive with a data breach costing an organization on average US$4.3 million (IBM/Ponemon Institute, 2022). At the same time, these costs can quickly grow exponentially and exceed US$100 million depending on the scope and length of the incident in question (ibid.).

The foundation of establishing robust cyber-security posture lies in the efficient management of individuals (Triplett, 2022). In fact, research has discovered that the consciousness component of users' behavior assumes a crucial significance, as numerous instances of cyber-security breaches can be attributed to poor user behavior such as a lack of knowledge, carelessness, limited awareness, malicious intent, indifference, and reluctance (Abroshan et al., 2021; Hong et al., 2023; Safa et al., 2015). Based on a systematic literature review, as many as 17 human factors have been identified impeding cyber-security measures (Rohan et al., 2021). Nevertheless, it is often overlooked that comprehending human behavior is imperative when addressing cyber-security concerns (Rahman et al., 2021; Triplett, 2022). Despite their regular utilization of the internet, a significant number of users exhibit a restricted understanding and proficiency in the realm of cyber-security. This encompasses even the younger, tech-savvy generation of individuals who have grown up with digital technologies and are skilled in their usage, comprising the so called "digital natives" (Bennett & Maton, 2010). In fact, research shows that the age group comprising "digital natives" often exhibits more risky online behavior and is thus exposed to a greater level of cyber-risk (Hancock, 2022; Hewitt & White, 2022; Kovačević et al., 2020; Rosoff et al., 2013). One of the reasons is that this group spends more time online and is therefore more frequently exposed to cyber-threats (Alanazi et al., 2022; Rosoff et al., 2013). However, another reason is that many of them simply still do not know how to properly protect themselves in the cyberspace (Kovačević et al., 2020; McGregor et al., 2023; Rodriguez-Priego & Bavel, 2023). For example, of nearly 30,000 individuals surveyed, a meager 23% refrain from accessing unsecured internet hotspots, and a mere 21% of respondents assert that they regularly change their passwords (European Commission, 2020). Likewise, only 39% of internet users know that the Internet Service Provider (ISP) can see the websites they visit in private browsing mode. Even though private browsing mode restricts the functionalities of the browser and ensures that data is not permanently stored on the user's device, it does not impede the ability of ISPs to track and monitor the transmitted information (Olmstead & Smith, 2017b). Furthermore, compounding the problem, some of the leading web browsers even fail to uphold satisfactory privacy measures after activating the private browsing feature (Ruiz et al., 2015). All these examples reinforces the lack of cyber-security awareness and need for more education (Olmstead & Smith, 2017b). While the variation in cyber-security knowledge among individuals is influenced by their age, the impact of these disparities is overshadowed by the differences associated with educational accomplishments. Indeed, research has found that individuals aged 65 and above possess a comparable level of knowledge in specific areas of cyber-security to those between the ages of 18 and 29 (ibid.). Other studies go even further, suggesting that older users significantly differ in their awareness of privacy issues and protect their data more actively than younger users (Zeissig et al., 2017). These results largely align with the findings of Wash and Rader (2015), indicating that individuals with higher levels of education are more inclined to believe that they are less susceptible to cyber-threats. This implies that education plays a significant role in shaping individuals' perceptions of online risks and their ability to safeguard themselves in the digital realm. Although effective cyber-risk mitigation heavily relies on individuals adopting safe online practices, a significant number of users continue to ignore even basic cyber-hygiene principles (Kostyuk & Wayne, 2020). Concurrently, the intelligence and sophistication of assailants are steadily advancing (Ament & Jaeger, 2017). They are skilled individuals possessing high levels of intelligence who exploit the lack of experience and naivety of the defenders or victims (Arief et al., 2015). Notably, even the experts in the field are facing mounting pressure due to the relentless onslaught of cyber-threats. Fewer than half (47%) of cyber-security leaders anticipate and understand the tactics deployed by attackers (EY, 2021).

The reality is that the internet never sleeps, and neither does crime. The susceptibility of individuals to certain behaviors makes them attractive targets for cybercriminals (Rodriguez-Priego & Bavel, 2023). At the same time, people need to make a myriad of decisions every day. The information available to individuals may affect their judgment. It causes them to commit errors due to various factors, encompassing the application of cyber-related heuristics and biases. Cognitive errors pose some of the most pernicious risks, yet their role within organizations remains largely misunderstood (Bone, 2021). Research has meanwhile identified more than 150 distinctively different cognitive distortions that may compromise the decision-making process (Dimara et al., 2018). Some researchers argue that there may be as many as 175 (Brooks et al., 2020) or even 187 (Eppler & Muntwiler, 2021) of these distortions. According to Johnson et al. (2020), over 87 of these biases, directly impact the actions and decision-making in the cyber-security domain. Noteworthily, the very top of the organization is not immune to judgmental flaws either. As highlighted in a recent survey, a significant majority of Chief Executive Officers (CEOs), specifically 96%, acknowledge the critical role that technology plays in their digital transformation strategy (Dal Cin et al., 2023). However, a considerable proportion of CEOs, almost 44%, do not consider cyber-security as a strategic business matter, indicating a stark disconnect (ibid.). There is also a risk that because of busy schedules, items are being overlooked or put on the backburner relative to other topics. Although nearly half (45%) of cyber-risk and technology leaders send information on cyber initiatives to their board, only a fraction of directors (18%) report to receive such information (Marsh/Microsoft, 2018). This information gap impedes gaining cyber-resilience and reduces risk exposure with many corporate directors swinging in the dark.

While the process of making cyber-security decisions bears resemblance to other types of decision-making, it possess certain unique characteristics since the cyber domain is vastly intangible and frequently imperceptible to users in the digital realm (Zimmermann & Renaud, 2021). Moreover, many of these decisions are of strategic nature given that these decisions are infrequent, complex, ambiguous, made under uncertainty, yet wide-ranging and potentially irreversible (Eisenhardt & Zbaracki, 1992; Schwenk, 1984). At the same time, when such decisions are taken lightly and subject to errors, the consequences in the cyber-context can be costly and potentially even devastating (Jalali et al., 2019; Qu et al., 2019; Rosoff et al., 2013).

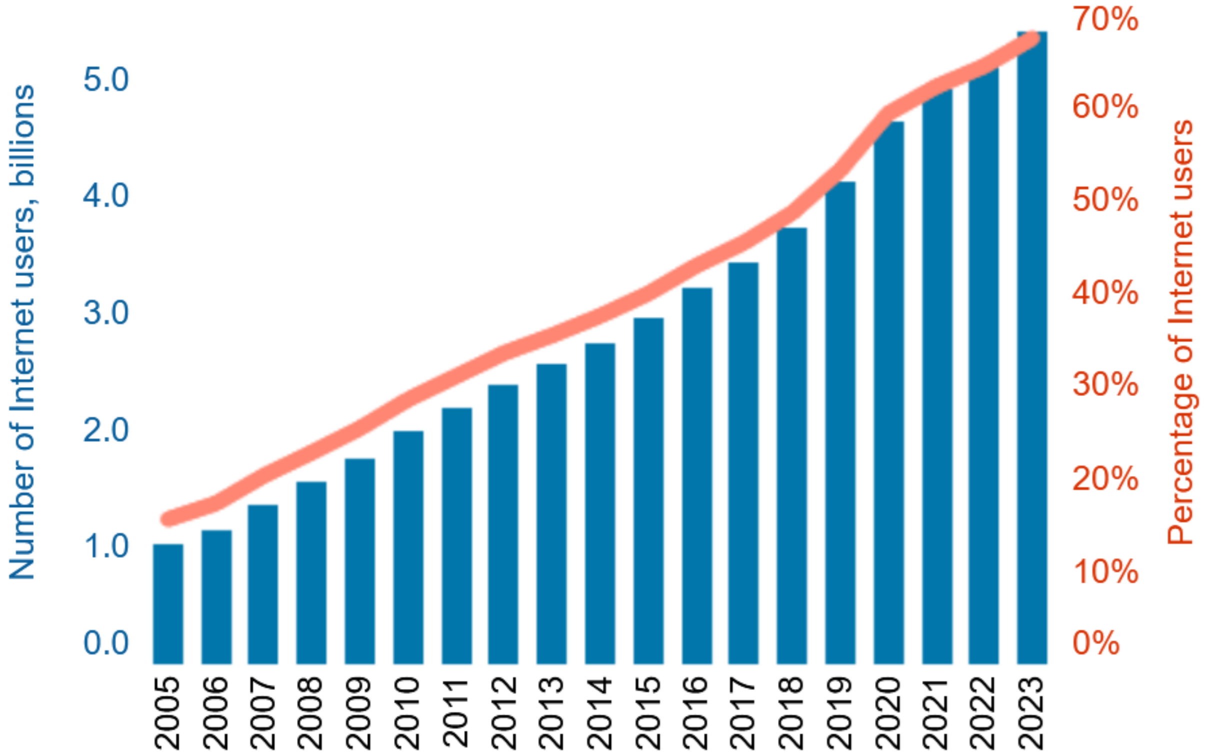
As established before, although effective cyber-risk management largely depend upon human behavior and human decision-making, limited research has been conducted thus far on the phenomenon of cyber-related *biases* and *heuristics* (Ceric & Holland, 2019; Sharma et al., 2021), particularly with emphasis on subject matter experts. This represents a novel field of studies (cf. Alnifie & Kim, 2023). On the back of global digitization efforts and increased connectivity, the internet plays a dominant role for commerce, trade, and other facets of life. Even critical infrastructure (such as power grids, smart cities, etc.) has interfaces into cyberspace, which makes it vulnerable to cyber-threats. This reinforces the importance of the subjects in question.

This thesis aims to explore the magnitude of cognitive distortions and their role in fostering erroneous judgments among cyber professionals. By examining these biases, the research seeks to equip cyber professionals with a deeper understanding of their decision-making processes, thereby enabling them to make more informed decisions and effectively reduce their organizations’ exposure to cyber-threats. Furthermore, this research is driven by the author’s personal curiosity about cyber-security, cybercrime, and the potential for mitigating biases that contribute to inefficiencies and provide fertile ground for the growth of cybercrime. Beyond achieving academic rigor, the ultimate goal of this research is to make a meaningful impact by supporting organizations in reducing their cyber-risk exposure and combatting the escalating threat of cybercrime.

1.2 Overview of Digital Transformation and Cyber-Security Threats

The global economy is at a pivotal moment of transformation. According to ITU (n. d.), the United Nations specialized agency for information and communication technologies (ICT), an estimated 5.4 billion people around the world, or around 67% of the global population, currently use the internet (see Figure 1). Internet users have grown by about 57% from 2017-2023, turning it into the fastest-growing multinational shared domain (Denić & Devetak, 2023).

Figure 1: Number of Global Internet Users



Source: ITU (n. d.)

The information-driven era is widely referred to as the "digital age." In 2006, Clive Humby famously labeled data as *"the oil of the 21st century."* This analogy illustrates the nature of data as a valuable input factor to fuel use cases and propel growth and prosperity in the digital economy (Mavuduru, 2020). Going forward, this trend is only going to accelerate. Within less than a decade, the number of connected Internet of Things (IoT) devices is expected to almost triple, growing from 11.3 billion in 2021 to 29.4 billion by 2030 (Transforma Insights, 2022). The growth of these IoT devices has not only already exceeded the human population on the planet, but it is also projected to soon outnumber it by approximately fourfold. In today's world, connectivity as well as the availability and integrity of digital services and communication networks go far beyond convenience. For instance, across the S&P500 Index, research has found that from 1975-2020, the impact of intangible assets on all business value has climbed from 17% to 90% with the emergence of the COVID-19 pandemic having further accelerated this trend (Ocean Tomo, 2020). This huge transformation has led to a situation where the assets of companies are predominantly stored in digital format within their corporate networks (Moore, 2010). Consequently, the cyberspace has turned into a paramount domain of power in the 21st century (Baldini et al., 2020; Li & Liu, 2021) and caused the foundations of our economy to change. Meanwhile, many of the world's most valuable companies operate platform-based business models underpinned by the internet (think Airbnb, Alibaba, Alphabet, Amazon, Baidu, eBay, Meta, Microsoft, Netflix, PayPal, Uber, and so on). In 2023, a significant milestone occurred as the Nasdaq 100 Index underwent an unprecedented transition, marked by the dominance of large Tech companies (collectively known as "Big Tech") which represent more than 50% of Nasdaq's overall market capitalization (Wang, 2023). This remarkable shift serves as a clear indication of the escalating dominance that these industry giants have established within the stock market, the global economy, and their impact on shaping the future. What all these companies have in common: being offline is just not an option. They need *uptime* like a human body needs oxygen with the same fatal consequences in the absence of it.

The reliance on the use of computers, technology and the internet has become an indispensable part of civilization. The huge adoption of digital technologies (otherwise known as *Digitalization*) has also transformed how people do business, communicate, and socialize with one another. In turn, many organizations are undertaking large digital transformation projects as established business models are reaching their end of life or are being heavily disrupted through technology-enabled new market entrants which realize efficiency gains and cost advantages. The adoption of digital technologies is becoming increasingly crucial for global economic growth and human well-being (Baldini et al., 2020). However, significant portions of the economy have previously underestimated both the opportunities and the risks associated with digital transformation (Bone, 2021). These initiatives promote better information exchange among stakeholders but also increase exposure to cyber-threats for the organization and its employees, customers, and suppliers (Loonam et al., 2022). In the digital age everything has gone online, including crime. Cybercrime has been on a constant rise and continues to emerge as a severe threat within the next years (Konradt et al., 2016). To underscore the growing severity of this threat, even the World Economic Forum (WEF) now lists the risk of cyber-attacks among the top-10 global risks over the next decade (see Table 1).

Table 1: Top-10 Global Risks ranked by Severity over the next 10 Years

Ranking	Risk
1.	Failure to mitigate climate change
2.	Failure of climate-change adaptation
3.	Natural disasters and extreme weather events
4.	Biodiversity loss and ecosystem collapse
5.	Large-scale involuntary migration
6.	Natural resource crises
7.	Erosion of social cohesion and societal polarization
8.	**Widespread cybercrime and cyber insecurity**
9.	Geoeconomic confrontation
10.	Large-scale environmental damage incidents

Source: WEF (2023b, p. 29)

Due to increasing digitalization around the globe, more so than ever “*individuals, organizations and governments alike are increasingly exposed to the risk and threats of the cybercriminals*” (Hunton, 2012). These cyber-attacks are becoming increasingly more targeted and persist in causing disruptions in various sectors, owing to a range of motives, including financial gain and political ideologies (Europol, 2023b). Indeed, economies and nation-states are amid a metamorphose toward a global informational economy, providing new opportunities that criminals utilize through the many forms of transnational organized crime (Sullivan, 2023). For example, 76% of the population across the European Union engage with the Internet daily (European Commission, 2020). Yet, there exists a limited awareness among individuals regarding the ramifications of their online conduct, with a scant number perceiving their actions as potentially hazardous (Rodriguez-Priego & Bavel, 2023).

In the United Kingdom, citizens are meanwhile significantly more likely to fall victim of cybercrime than experiencing a car theft or domestic burglary (Cook et al., 2023). The COVID-19 outbreak, and lockdown restrictions have further accelerated this trend consistent with overall increased online activity during the pandemic (Duong et al., 2022; Lallie et al., 2021). Across multiple dimensions, from home schooling to remote work or purchases, people had no other choice than to adapt their daily routine and go online. This notable surge in online communication during the COVID-19 pandemic was accompanied by a substantial rise in malicious cyber activities (Saleous et al., 2023). The implementation of social distancing measures has accelerated the exploration of novel approaches to foster collaboration, learning, and social engagement (Bhatt & Shiva, 2020; Kagan et al., 2020; Nuryana et al., 2021).

Likewise for organizations, the outbreak of the COVID-19 pandemic translated into a *Black Swan* event, forcing them to radically improvise, implement new digital technology at rapid speed and embrace remote work, sometimes by making cyber-security an afterthought.[1] Consequently, as much as the COVID-19 pandemic opened more doors for users to access the cyberspace, it introduced an equally large opportunity for threat actors to capitalize on it (Duong et al., 2022). There has also been a positive correlation effect between imposing strict lockdown measures and a spike cyber-related crimes such as online fraud, and the breach of social media and e-mail accounts (Buil-Gil et al., 2021). While some level of crime would have been conducted anyway, specifically cybercrime witnessed a noticeable surge during the COVID-19 pandemic (Chigada & Madzinga, 2021; Cook et al., 2023; Europol, 2022; Pranggono & Arabo, 2021). The results of these studies align with the observations made by the Federal Bureau of Investigation (FBI), which documented a 300% surge in the incidence of cybercrimes amidst the pandemic (Miller, 2020). These observations extended across a wide range of different attack techniques including cyber-related fraud (Levi & Smith, 2021), DDoS attacks (de Neira et al., 2023), phishing (Abroshan et al., 2021; Al-Qahtani & Cresci, 2022) and ransomware (Alqahtani & Sheldon, 2022; Duong et al., 2022). There have also been instances recorded of cyber-attacks perpetrated by criminals masqueraded as World Health Organization (Baldini et al., 2020). These findings are consistent with previous research, implying that a higher internet usage introduces a higher risk of witnessing cybercrime (Choi, 2008; Pratt et al., 2010).

Although offenses like burglary and assault are more conspicuous, cybercrime predominantly operates in secrecy, causing a significant number of individuals to undervalue its true impact and the probability of falling prey to it (WEF, 2020). In the terrestrial world, most offenses are perpetrated near the offender’s home. Criminals only make the effort to travel far if it merits sufficient incentives (Van Koppen & Jansen, 1998). Cybercrime in that sense has made it even more comfortable for criminals and lowered the barriers to commit offenses since it can be largely conducted from a distance. The technological shifts in recent years have opened pathways for offenders to commit crimes in the digital realm (Ouellet & Dubois, 2022), and allows them to remotely strike around the globe. This is consistent with observations by the United Nations Office on Drugs and Crime, stating that the increased use of the internet is

[1] In 2001, Nassim Nicholas Taleb, a mathematician and Professor of Risk Engineering at the New York University Tandon School of Engineering, introduced the *Black Swan Theory*, suggesting that unforeseen disruptive events can cause far-reaching consequences, and are often inappropriately rationalized after the fact with the benefit of hindsight.

indeed creating new opportunities for criminals and may fuel the growth of crime. For example, some individuals show differences between their *conforming* (legal) and *non-conforming* (illegal) behavior and might commit crimes in cyberspace that they would not commit in the physical world (UNDOC, 2013). Even the increased availability of internet broadband combined with higher inequality, that is, higher education and higher income, has further stimulated cybercrime (Noroozian et al., 2016; Park et al., 2019). These findings challenge conventional notions of crime, as they indicate that poverty does not necessarily play a significant role as a motivating factor.

In sum, the prevalence of cybercrime has reached unprecedented levels, making it one of the foremost profit-driven criminal activities across the United Kingdom (Office for National Statistics, 2022; Scottish Government, 2021; Williams et al., 2019), Ireland (Central Statistics Office, 2020) and Spain (Kemp et al., 2020), and elsewhere across the European Union (Armin et al., 2015). Cyber-attacks continued to increase during the second half of 2021 and 2022, not only in terms of attack types and numbers but also in terms of their impact (ENISA, 2022a, p. 8).[2] In fact, about half of all property-related crime, by volume and by value, is now committed online (Anderson et al., 2018). According to Europol, perpetrators continue to be increasingly ruthless and methodical in their *modus operandi* (Europol, 2022, p. 8).

On a micro-level, cyber-threats pose severe corporate risks, including business disruption, productivity loss, breach of privacy, erosion of trust, reputational damages, customer churn and financial losses (Arief et al., 2015; Farahbod et al., 2020; Sheehan et al., 2019). Along with digital transformation, IT moves from a support function to the core of the firm and now builds the foundation for revenue and profits. In today’s business environment, digital technology has become an essential source of competition with data being the currency. Despite its resemblance to a Darwinian struggle, like the gnus facing the perilous river crossing, companies are caught between a rock and a hard place and have limited alternatives for their advancement. Without technological adoption, organizations risk falling behind and struggling to keep pace with changing market dynamics (cf. Peppard & Ward, 2016, p. 167). Rival companies will continuously strive to discover more efficient and superior methods to satisfy their customers. This causes a real dilemma and has wide-ranging implications for companies

[2] Although the term cyber-attack is widely used in the public, media, by governments and among academia, there is ambiguity as to what constitutes a cyber-attack. Cyber-attack is a hypernym since such attacks can take many forms and variants. For the present purpose, cyber-attack shall therefore refer to any malicious action in the cyberspace or against related equipment or individuals causing damage.

as it inevitably makes them more susceptible to cybercrime while exponentially growing the material implications of a successful cyber-attack.

On a macro-level, on the back of digitalization, societies have radically increased their reliance on the availability and integrity of information and communication technologies (ICT). Consequently, cyber-attacks can have devastating consequences far beyond just an individual firm which turns cyber-threats into a *systematic risk*, posing a danger to propagate across interdependent systems and entities (Schwarcz, 2008; Welburn & Strong, 2022; Wilson et al., 2019).[3] For example, the International Monetary Fund (IMF) notes, that the *"cyber-threat landscape is highly dynamic and rapidly changing. The nature of cyber-attacks and threat actors continue to evolve. Attacks against ICT systems have the potential to endanger financial stability"* (Wilson et al., 2019). Especially spill-over effects have the risk of impeding critical infrastructure, crippling a nation's entire economy, and instigating panic and wide-ranging economic damages. With respect to international relations, the proliferation of cyber-threats has disruptive and destabilizing effects (Sviatun et al., 2021). At the same time, cyberspace has witnessed a noticeable surge in the involvement of state-sponsored actors and rogue nations amidst rising geopolitical rivalry and tensions, aggravated by a trend toward decoupling and deglobalization. The scope of their operations encompasses a wide range of activities, undermining national security and diplomatic relations. In reflection of a surge of attacks coupled with huge investments made by nation states to build both defensive and offensive cyber capabilities, some experts have referred to this paradigm as the rise of a "digital arms race" within the cyberspace (Craig & Valeriano, 2016; Goel, 2020). Particularly, authoritarian regimes across the globe are seeking to gain control. According to the Center for Strategic and International Studies (CSIS), especially Russia, North Korea, China and Iran have emerged as severe threat actors causing havoc (Lewis, 2018). North Korean actors are primarily driven by financial incentives to aid the Pyongyang regime, whereas Russian APT groups are also involved in disseminating propaganda and aggressively promoting the Kremlin's agenda (Andrew et al., 2015; Blackwill & Gordon, 2018; Kadlecová, 2015; Kim, 2022). The meddling in various election processes serves as a mere glimpse of a much more complex problem. China, on the other hand, has taken the lead in engaging in espionage activities (Kshetri, 2013; Lewis,

[3] There is no single, widely accepted definition of systemic risk. What most definitions have in common is that a trigger event causes a chain reaction leading to a short-term economic shock or institutional failure. For present purposes, a systematic risk will be considered as a wide-ranging risk causing failures or negative effects inherent to the entire market or market segment.

2018). In contrast, Iran has demonstrated its inclination to exert coercive influence by initiating distributed denial-of-service (DDoS) attacks on prominent American banks (U.S. Department of Justice, 2016) and by targeting the ICT space (CISA, 2021c).

The manifestation of these tectonic changes causes a transformation in the core principles of cyber-security, demanding a comprehensive reassessment of the existing approaches and measures in place. Research on technological aspects of cyber-risk is a well-established discipline and familiar terrain for cyber-security practitioners. However, despite this huge uptick of cybercrime, little academic research has thus far scrutinized the economic implications resulting out of the above (Cook et al., 2023; Holt, 2017; Schatz & Bashroush, 2017; Sheehan et al., 2019). Economic concepts can be employed to offer a more lucid and convincing elucidation for a plethora of cyber-security concerns. This encompasses a range of factors including *adverse selection*, *information asymmetries*, *liability dumping*, *moral hazard*, *network externalities*, and *the tragedy of the commons* (Anderson, 2001). While rationality is a desirable trait in decision-making, it is important to acknowledge that humans are not always purely rational agents. The effectiveness of understanding and addressing decision-making in the cyber-security domain can therefore be greatly enriched by considering them through the lens of behavioral economics.

1.3 Research Objectives

As we transition from the broader context of cyber-risks and the impact of digital transformation, it becomes increasingly clear that addressing these challenges requires a deeper understanding of human behavior. The effectiveness of cyber-security measures is heavily dependent on the pivotal role that humans play, given the unpredictable and varied nature of their behavior and actions (Lahcen et al., 2018). Much like other areas of strategic decision-making, decisions related to the disclosure of information or ensuring cyber-security can be influenced by cognitive and behavioral biases (Acquisti et al., 2017; Leon et al., 2012). These biases are characterized by consistent deviations in judgments and actions that differ from what a rational decision maker, aiming to maximize their *utility*, would typically choose (Acquisti et al., 2017). The examination of cyber-security behavior has witnessed a noteworthy influx in scholarly publications lately, particularly during the years 2019, 2020, and 2021 (Alsharida et al., 2023). Meanwhile, there exists a broad agreement in contemporary research that comprehending the cyber-security behaviors of humans is crucial in identifying the measures and factors that can effectively reduce cyber-risks exposure (e.g., Alanazi et al., 2022; Alnifie

& Kim, 2023; Alsharida et al., 2023; Balebako & Cranor, 2014; Bone, 2016, 2021; Ceric & Holland, 2019; Hartwig & Reuter, 2021; Hewitt & White, 2022; Zimmermann & Renaud, 2021). However, research in this field is still nascent and demands a deeper examination and inquiry (Lahcen et al., 2018; Maalem Lahcen et al., 2020). Furthermore, according to a systematic literature review (SLR) carried out by Alsharida et al. (2023), the bulk of the work in this area is still vastly focused upon regular users including students and employees (see e.g., Alanazi et al., 2022; Hewitt & White, 2022; Sharma et al., 2021; White, 2015), and to a much lesser extent on IT professionals let alone cyber-security professionals. Of the 2,936 articles collected by Alsharida et al. (2023), 93 studies on human cyber-security behavior were reviewed. Notably, 86% of these articles concentrated on non-IT professionals, despite the critical role that IT and cyber professionals play in an organization's cyber-security posture. This imbalance suggests that the unique needs and behaviors of those who are directly responsible for cyber-security are being overlooked, which could undermine the efficacy of mitigation strategies and reveal a significant vulnerability.

The aim of this dissertation is to explore the challenges and limitations in cyber-related strategic decision-making processes, particularly under conditions of bounded rationality. The analysis will primarily be guided by the principles of behavioral economics, with a particular focus on cognitive biases and heuristics. Cognitive biases refer to the systematic errors in thinking that individuals tend to make, often resulting from limited rationality. These biases can lead to distorted risk perception, where individuals either underestimate or overestimate the likelihood and impact of cyber-threats. This inaccurate risk perception then leads to inadequate risk mitigation strategies, leaving organizations vulnerable to cyber-attacks. Heuristics, on the other hand, are mental shortcuts or rules of thumb that individuals use to make decisions quickly and efficiently. While *heuristics* can be useful in certain situations, they can also lead to *biases* and errors in judgment. In the context of cyber-security, *heuristics* can lead decision-makers to rely on outdated or incomplete information, leading to suboptimal strategic decisions.

By shedding new light on the emotional and cognitive aspects of decision-making, the aim is to provide a deeper understanding of how these factors impact cyber-security strategies. To achieve this objective, the research will explore various research inquiries that aim to counter or reduce the influence of cognitive biases on cyber-related strategic decision-making. These inquiries may include examining the role of emotions in decision-making, investigating the impact of cognitive biases on risk perception, and exploring strategies to mitigate the influence of heuristics on decision-making.

With that in mind, the research objectives are to (i) investigate the significance of biases and heuristics affecting strategic decision-making in cyber-related questions as it relates to IT professionals and cyber-expert across mid-market companies and large-enterprises in Germany, Austria, and Switzerland; (ii) evaluate specifically how cognitive biases such as *optimism, overconfidence,* and the *availability heuristic* lead to distortions in the assessment of cyber-threats, the implementation of safeguards, and the mitigation of cyber-attacks; (iii) study the emergence of cybercrime including the supporting elements and threat actors exacerbating the situation and ultimately exposing organizations to cyber-threats; (iv) examine and contextualize the cyber-risk landscape and illustrate the economic consequences of flawed decision-making; (v) close the theoretical gap in existing literature when it comes to cyber-related biases; and (vi) provide practical advice to practitioners what action can be taken to make more informed decisions and derive at better outcomes to reduce their organization's cyber-risk exposure.

1.4 Research Questions

The research objectives of this thesis are framed around three primary research questions that address the complexities of cyber-security decision-making, the proliferation of cyber-threats, and the economic consequences of cyber-security incidents. To address these questions comprehensively, the thesis employs a combination of theoretical and empirical research.

RQ1: When it comes to cyber-related questions, what are the cognitive biases that hinder subject matter experts in their decision-making and impact the effectiveness of countermeasures?

As highlighted in the introduction, there is broad consensus in current research about the increasing severity of cybercrime and the significant consequences of cyber-security incidents (see e.g., Kianpour et al., 2021; Nikkhah & Grover, 2022) as well as the far-reaching material consequences that result from cyber-security incidents and breaches (Bernik, 2016; Hancock, 2022; IBM/Ponemon Institute, 2022; Jeong et al., 2019; Sviatun et al., 2021; WEF, 2023a). This malicious trend is not expected to change anytime soon (Alnifie & Kim, 2023). Despite the widespread recognition of these threats, inconsistencies remain between the perception of cyber-threats and the measures organizations implement to address them (e.g., Alsharida et al., 2023; Dal Cin et al., 2023; Ting, 2019). This inconsistency calls into question the effectiveness of current risk management practices and highlights how cognitive biases may contribute to a false sense of security. Such biases can lead experts to underestimate the likelihood of cyber-threats or overestimate their capacity to handle them, ultimately leaving organizations more vulnerable to attacks.

To answer this question, the research adopts a multi-method approach, integrating both qualitative and quantitative methodologies to offer a comprehensive understanding of cognitive biases in cyber-security decision-making.

Chapter 2 establishes a theoretical framework by exploring key cognitive biases, such as *overconfidence* and *optimism bias*. This framework provides context for understanding how these biases distort judgment and impact risk management strategies.

To refine the focus on specific biases, the study includes qualitative research involving interviews with leading cyber-security experts. These interviews are carefully transcribed and coded to reveal how biases manifest in real-world decision-making. This qualitative phase ensures that the empirical analysis addresses the most relevant biases and provides a nuanced understanding of how these biases affect cyber-security practices.

Building on the insights gained, Chapter 6 employs a robust empirical approach to examine the relationships between identified biases and cyber-security outcomes. Using quantitative methods, the study analyzes how biases, including *overconfidence* and *optimism bias* and the presence of an *availability heuristic*, influence experts' perceptions of risk and their decision-making processes in real-world scenarios. This approach allows for a structured examination of how biases affect cyber-security practices, providing quantifiable evidence of their impact.

By integrating theoretical exploration, qualitative insights, and empirical analysis, this research offers a comprehensive understanding of how cognitive biases impact cyber-security decision-making. This approach ensures that the findings are rooted in both practical experience and theoretical knowledge, leading to more robust and actionable insights into improving risk assessment and management practices.

RQ2: What are the driving forces behind the proliferation of cyber-threats, and how do cognitive biases shape the effectiveness of countermeasures in the evolving cybercrime landscape?

Despite substantial investments in cyber-security in recent years, cybercrime continues to thrive (Cremer et al., 2022; Demirdjian & Mokatsian, 2015; Fielder et al., 2018; Kianpour et al., 2021; Nikkhah & Grover, 2022). As established before, the surge in digital engagement, especially during the COVID-19 pandemic, has provided cybercriminals with more opportunities to exploit vulnerabilities. The repeated dismantling of criminal syndicates and illegal marketplaces on the Dark Web by law enforcement had little effect (Denić & Devetak, 2023; Wang et al., 2023), and cyber-related damages continue to surge (Demirdjian & Mokatsian, 2015; Europol, 2022; IBM/Ponemon Institute, 2022; Nikkhah & Grover, 2022). In particular, the emergence of Cybercrime-as-a-Service (CaaS) is denoted as a "critical evolution" in the cyberspace (Akyazi et al., 2021) and a "sustained business" (Nobles et al., 2023), which has a significant impact on the threat landscape (Huang & Madnick, 2017; Huang et al., 2018). To contain cyber-threats and mitigate cyber-risks, it is essential to understand the different threat actors and their motivations to derive effective measures (Jakobi, 2013; Ouellet & Dubois, 2022). This includes analyzing how technological advancements and the commercialization of cybercrime contribute to its growth. In spirit of Sun Tzu, regarded as one of the founding fathers of military strategy, and his seminal work, *The Art of War*, one must "know the enemy". Conversely, not knowing whom organizations are up against in cyberspace makes the definition and implementation of counteraction ineffective.

To address this inquiry, the thesis will adopt a multi-faceted approach, beginning with a comprehensive literature review that traces the evolution of cybercrime. In extension of Chapter 1, which outlined the growing prevalence of cybercrime amidst increasing digital engagement, Chapter 3 will provide a theoretical foundation by examining the progression of cybercrime, with a specific focus on technological advancements and the impact of business models like CaaS on the cybercrime ecosystem. This chapter will also explore the dynamics of the Dark Web and the persistence of illegal marketplaces, highlighting the challenges law enforcement faces in curbing these activities.

Chapter 4 will delve into the various threat actors involved in cybercrime, ranging from individual hackers to state-sponsored groups, and their supporting infrastructures. This chapter will analyze the motivations behind these actors, such as financial gain, political objectives, and ideological drives, which fuel the continued proliferation of cyber-threats. By identifying the key drivers behind the growth of the cybercrime ecosystem, this chapter aims to provide insights into the complex interplay of factors that sustain these threats.

Further, Chapter 5 will examine the dual role of digital technology in both enabling cybercrime and increasing vulnerabilities. This chapter will explore how digital advancements have expanded the attack surface, facilitating more frequent and severe cyber-attacks, particularly on critical infrastructure. The *spillover effects* of these attacks and the broader implications for global cyber-security will be assessed, contributing to a more holistic understanding of the cybercrime ecosystem.

Finally, Chapter 6 will integrate the empirical findings of this thesis, focusing on the effectiveness of current countermeasures against cyber-threats. The analysis will highlight how cognitive biases, such as an *availability heuristic, overconfidence* and *optimism bias*, may undermine these efforts, leading to underinvestment in necessary cyber-security measures. By correlating these biases with the observed proliferation of cybercrime, the chapter will provide evidence-based insights into the shortcomings of current strategies and suggest potential avenues for more effective interventions.

RQ3: How are the economic consequences of cyber-security incidents underestimated due to cognitive biases, and what are the broader implications for businesses and societal resilience?

Despite the increasing cyber-threats and risks, the consequences are still widely underestimated (e.g., Armin et al., 2015; Dal Cin et al., 2023; Rodriguez-Priego & Bavel, 2023; Ting, 2019). Especially considering further digitization efforts, the dependencies regarding the availability and integrity of the cyberspace are growing (Brar & Kumar, 2018; Singh & Bakar, 2019; Vagle, 2020a). With the increasing number of users and the shift of business models to the cyberspace, as well as its influence in various aspects of life, far-reaching economic consequences can be expected in cases of data breaches, outages, and attacks (Crosignani et al., 2023; Li & Liu, 2021; Lis & Mendel, 2019; Welburn & Strong, 2022).

In addressing this question, the study employs a comprehensive literature review alongside empirical analysis to identify the factors that lead to the underappreciation of the economic repercussions stemming from cyber-security incidents. The methodology is structured into several critical phases.

Chapter 3 lays the groundwork by exploring the economic ramifications of cyber-security incidents, delving into aspects such as cyber-politics, deterrence, established norms, and the financial burdens associated with cybercrime, particularly the role of CaaS in shaping the economic environment. This chapter is essential for grasping the intricate nature of cyber-risk and its fiscal implications.

Chapter 4 shifts focus to the diverse array of cyber-threat actors, including state-sponsored entities and organized crime groups. It scrutinizes how these actors amplify the overall economic effects of cyber-security incidents by investigating their operational methods, underlying motivations, and the supporting infrastructure that enables their activities.

Chapter 5 centers on the themes of cyber-risk management and resilience, particularly concerning digital technologies and vulnerabilities within critical infrastructure sectors. It underscores the persistent challenges in effectively managing cyber risks and evaluates how these challenges affect the economic fallout from cyber-security incidents.

Chapter 6 offers empirical insights into the economic consequences of cyber-security incidents, examining the disparity between perceived and actual risks while pinpointing the elements that contribute to the underestimation of economic impacts. Through data analysis and empirical research, this chapter elucidates the financial ramifications of cyber-security incidents and their broader implications for both businesses and society.

By synthesizing theoretical frameworks with empirical findings, this research provides a holistic perspective on the reasons behind the underestimation of the economic consequences associated with cyber-security incidents, culminating in actionable recommendations for stakeholders.

1.5 Method

The research adopted a blended approach, integrating both qualitative and quantitative methods to offer a comprehensive and nuanced analysis of the research topic. Given that the proliferation of cybercrime is a relatively recent phenomenon, especially from an economic perspective, research in this area remains scarce. Consequently, while this thesis primarily examines the subject through an economic lens, it is inherently interdisciplinary, drawing upon insights from social sciences (including criminology and psychology), political science, and computer science. This interdisciplinary approach provides a well-rounded perspective on the complexities of the issue, enriching the discourse and enhancing the study's overall depth.

The research commenced with an extensive literature review and critical analysis across several domains, including behavioral economics, decision-making under uncertainty, and the role of cognitive biases in cyber-security. This review was pivotal in contextualizing the research within the broader landscape of strategic decision-making and identifying key areas where cognitive biases may influence outcomes. It also provided a foundation for the subsequent qualitative and quantitative phases of the study. As the research progressed, expert interviews helped systematically narrow this scope, using Kuckartz's (2014) structured content analysis. The staged approach identified three main patterns—*availability heuristic, optimism*, and *overconfidence*—ensuring the research remained aligned with its title while focusing on specific biases of interest. The quantitative phase involved the development of a tailored questionnaire, with the collected data analyzed using Structural Equation Modeling (SEM) and SPSS. This phase specifically focused on empirically examining the three identified judgmental errors within a high-quality dataset of cyber professionals, ensuring that the research title's broad promise was fulfilled through a methodical narrowing and empirical exploration of key biases. Detailed methodologies are discussed in Chapter 6.

Finally, a comprehensive set of recommendations derived from the research findings was presented. These suggestions, along with an elucidation of constraints, contributed to enhancing the overall credibility and reliability of the research outcomes and facilitated future investigations in the field. By linking theoretical perspectives with empirical data, the thesis aims to provide a comprehensive understanding of how cognitive biases affect decision-making in cyber-security and to suggest strategies for mitigating their impact.

1.6 Structure of the Thesis

Following the introduction (Chapter 1), Chapter 2 elucidates the field of behavioral economics. In addition to providing an outline of the topic and a summary of the important research, this study delves into the specific heuristics and their practical implementation in relation to cyber-related aspects. Special consideration is given to the fact that decisions are often made under less-than-ideal circumstances and the impact of cognitive biases on the decision-making process. Some judgmental errors are exemplified in the context of cyber-security, demonstrating how these biases can lead to suboptimal outcomes and ultimately increase the risk of a cyber-security incident.

Next, Chapter 3 discusses the cyber domain. It begins with an overview of the foundations, including Information and Communication (ICT) technology and cyberspace, and proceeds to elaborate on the politicization of cyberspace (“cyberization”) before addressing cybercrime and cyberwarfare. Furthermore, the business model of CaaS, the cybercrime ecosystem, and criminal value chains are examined. Special attention is given to the dynamics of the Dark Web, the rise of illegal online marketplaces, and the efforts of law enforcement agencies to combat these activities and apprehend the perpetrators. Additionally, it elaborates on the motives of threat actors, the economic damage caused by cybercrime, and the aspect of the criminal darkfield.

The subsequent section (Chapter 4) sheds light on the cyber-threat landscape. In addition to providing a general overview of various cyber-threats, particular attention is given to the emergence of ransomware. Two global ransomware campaigns are exemplified, along with the resulting economic consequences. Furthermore, the different threat actor types and their capabilities, as well as the influence and threat posed by hostile state actors, are explained. Finally, the underlying and supporting infrastructure utilized by cybercriminals is discussed, highlighting how these actors establish and operate their illegal business models while employing tactics of obfuscation to evade law enforcement.

The forthcoming section (Chapter 5) investigates the topics of cyber-risk and cyber-resilience. Additionally, the chapter addresses the dual nature of digital technology, shedding light on its positive and negative aspects. Furthermore, the discussion extends to the *spillover effects* that arise from the utilization of digital technology, as well as the potential vulnerabilities it exposes in critical infrastructure.

Chapter 6 establishes the theoretical foundation for the study, focusing on the complexities of decision-making in cyber-security. It delves into misconceptions and psychological barriers that impede effective decision-making, as well as the financial implications of these challenges. Key issues such as counterfactual thinking, measurement error, and the risks associated with cyber exposure are explored. Additionally, organizational barriers that hinder cyber-security efforts are discussed, culminating in a summary that highlights existing research gaps and integrates these insights with current literature. The chapter also outlines the empirical research methodology employed in the study. It begins with background interviews to provide context, followed by the design and execution of a detailed questionnaire. The empirical analysis is then presented, including a review of sample demographics and an introduction to the SEM. This model is used to examine the broader relationships between key constructs. The results are synthesized to validate the study's findings, with supplementary analyses exploring group differences. The chapter concludes by acknowledging the study's limitations and offering recommendations aimed at enhancing decision-making processes in cyber-security.

In sum, the structure of can be envisaged as illustrated below (see Figure 2).

Figure 2: Design of the Thesis

Chapter 1	Motivation, Introduction & Background		
Chapter 2	Evolution of Rationality and Biases in Economic Thought		
Chapters 3-5	Cyber Realm including Cyberspace, Cybercrime and Cyber Warfare	Cyber-Threat Landscape including Threat Actors and their supporting Infrastructure	Cyber-Risks and Resilience including Spillover Effects and Critical Infrastructure
Chapter 6	Theoretical Framework, Empirical Research, and Research Insights		

CHAPTER 2
THE EVOLUTION OF RATIONALITY AND BIASES IN ECONOMIC THOUGHT

2.1 Introduction

Behavioral Economics (BE) is a branch of economics and a relatively new field of study that has emerged from the intersection of psychology and economics. Despite being considered “new”, its origins date back to the classical school of economic thought—especially to the contributions of Adam Smith. However, classical economics (CE) assumes that people behave *rationally* in all economic decisions and there is *information symmetry* among individuals. Problems and costs that may arise when obtaining information are completely ignored. Uncertainties that lie within a contractual partner (e.g., default risks) are also disregarded in classical economics.

The neoclassical economic (NE) theory attempts to address some of the limitations of classical economic theory, focusing primarily on the allocation of scarce resources. Consumers possess specific needs and aspire to attain the utmost personal benefit by means of *utility*. Diverging from CE, NE employs the notion of *marginal productivity* and *marginal utility*, while accentuating the significance of price in establishing *market equilibrium*.

Institutional economics (IE), an economic school of thought that originated in the United States towards the end of the 19th century, examines the interplay between the economy and societal institutions. It is crucial to differentiate this approach from the more recent development of new institutional economics. The latter places significant emphasis on the analysis of institutions that govern the economic exchange of services, encompassing markets, organizations, and legal norms. *Transaction costs* introduced by Ronald Coase, or the minimization thereof, play a pivotal role in the establishment and perpetuation of these institutions.[4]

[4] Ronald Harry Coase (1910-2013) was a British economist and professor at the Universities of Buffalo, Virginia, and Chicago. In recognition of his groundbreaking contributions, he was awarded the Alfred Nobel Memorial Prize in Economics in 1991. Coase's remarkable achievement lies in his profound exploration and elucidation of the pivotal role played by transaction costs and the rights of disposal in shaping the institutional structure and operational dynamics of the economy. This seminal work, commonly referred to as the *Coase Theorem*, has significantly advanced our understanding of economic principles.

The new institutional economics diverges significantly from NE theory, which is based upon a simplistic model of a rational *homo economicus*, thereby ignoring transaction costs and non-economic *behavioral incentives*. Neo-institutional (NI) economists argue that this assumption is unrealistic, as it distorts the reality wherein transaction costs and non-economically motivated behavior hold great importance. NI economics endeavors to develop a realistic behavioral model that considers a multitude of potential influencing factors on human actions. Moreover, it seeks to incorporate the fundamental aspects of human behavior, such as instincts, natural needs, and other innate behavioral dispositions, to comprehend their significance in economic decision-making. Notable examples encompass *principal-agent conflict*, *moral hazard*, and *bounded rationality*. In contrast to classical and neoclassical economics, the new institutional economics acknowledges the behavior of economic actors, yet it fails to address numerous inquiries regarding actual market behavior. Consequently, there is a dearth of understanding regarding how market participants form their preferences or the circumstances that contribute to irrational decision-making.

Rationality has long been a contentious issue in economics. NE is founded on the assumption that individuals act as *homo oeconomicus*, characterized as self-interested rational agents, seeking to maximize their preferences, and making “optimal” decisions. Empirical research applying a BE perspective has challenged this assumption, revealing that real-world decision-making is frequently influenced by cognitive biases, emotions, and limited information, leading to deviations from purely rational behavior. BE aims to address these shortcomings by focusing on how these deviations occur, emphasizing the limits of rationality and the impact of biases on economic decision-making.

As outlined before, the origins of BE can be traced back to the founding fathers of economics including Adam Smith. Smith is mostly remembered for his groundbreaking book *An Inquiry into the Nature and Causes of the Wealth of Nations*, published in 1776, and the concept of the invisible hand, that describe how free markets incentivize rational agents and guides an economy toward prosperity. However, he also acknowledged the prevalent tendency of individuals to exhibit behavior that is not purely rational and self-interested. In his first book, *The Theory of Moral Sentiments*, published in 1759, Smith describes important aspects that have been subject to scientific scrutiny and analysis within the field of behavioral economics from the 1950s onward. For instance, Smith touched upon “overweening conceit”, willpower, and loss aversion (Ashraf et al., 2005). Indeed, it can be argued that Smith was a pioneer in the field of BE. The notions described by him, namely overconfidence, loss aversion, and self-control, have all become fundamental principles within the realm of behavioral economics.

Similarly, in his manifest named *Manual of Political Economy* released in 1906, Vilfredo Pareto underlined the importance of the interplay between economics and psychology.[5] More specifically, right at the beginning in his opening section he stated that *"the foundation of political economy and, in general, of every social science, is evidently psychology. A day may come when we shall be able to deduce the laws of the social science from the principles of psychology, in the same way that someday, perhaps, the principle of the constitution of matter will give us, by deduction, all the laws of physics and chemistry"* (Pareto, 2014).

Nearly half a century following Pareto's prophecy, he was finally proven right, and psychology slowly but surely made its way into the field of economics and justified its "right to play." While some scholars welcomed the paradigm shift and acknowledged the need to look beyond the notion of strict rationality, others viewed these advances more controversially.

The subsequent sub-chapters will explore various behavioral economic theories and their relevance to decision-making. Additionally, this section will provide an overview of key biases and heuristics, highlighting their specific role in the decision-making process within the cyber domain.

2.2 Rational Choice

Rational choice (otherwise referred to Rational Choice Theory or RCT in short) is a theoretical approach that is widely employed in various disciplines across the humanities and social science to elucidate and *rationalize* the behavior of hypothetical actors in social, political, or economic decision-making scenarios. The central focus of the theory is on the decision-making processes of individuals who carefully evaluate their alternatives and ultimately select the option they believe will be most advantageous to them under specific situational conditions. The determination of what constitutes the optimal choice is contingent upon an individual's personal preferences. The likelihood of an action being undertaken is directly proportional to the personal benefits associated with it and inversely proportional to the personal costs incurred. In economic terms, the individual strives to *maximize* his or her *utility* of the actions taken. However, according to Gary Becker, it is evident that individuals do not consistently exhibit

[5] Vilfredo Federico Damaso Pareto (1848-1923) was an Italian polymath, excelling in various fields such as civil engineering, economics, philosophy political science, and sociology. His notable contributions to economics are centered around the examination of income distribution and the analysis of individual decision-making.

rational behavior under certain conditions.[6] Thus, the term "rational" does not inherently disregard or explicitly acknowledge the reality that decisions are often made amidst incomplete information, a lack of transparency, and uncertainty regarding expectations. Consequently, such decisions may also encompass biases (Becker, 1962, 1976). In fact, Becker highlighted: *"Indeed, perhaps the main conclusion of this study is that economic theory is much more compatible with irrational behavior than had been previously suspected"* (Becker, 1962). The subsequent experimental findings of behavioral economics (see e.g., Thaler & Mullainathan, 2001; Thaler, 1980; Tversky & Kahneman, 1974; Tversky & Kahneman, 1979, 1981) have posed significant challenges to Rational Choice Theory.

In criminology, this general action-theoretical model of *rational choice*, which was also proposed in the classical economic school of thought, has been utilized to explain the phenomenon of crime or deviance. Accordingly, the probability of a delinquent act increases if the benefits of such an act outweigh the costs, such as when the potential gains from the crime are deemed to be greater than the risk of being caught. This observation is of particular significance as the motives of cybercriminals will be further explored during this thesis (see Chapter 3.3.5).

2.3 Strategic Decision-Making

Strategic decisions encompass a collection of paramount choices that management undertakes, constituting the *"cornerstone of strategy"* (Schrager & Madansky, 2013). At the same time, management is faced with major challenges when making such decisions. Such strategic decisions are not only characterized by a lack of structure, they are also *"important, in terms of the actions taken, the resources committed, or the precedents set"* (Mintzberg et al., 1976). Decision-makers initially possess limited comprehension of the given situation, and thus make their judgement subject to *bounded rationality*. These decision-makers only gradually gain an understanding as they engage in problem-solving activities and advance through the process (Schwenk, 1984). Rationality is also contingent to other parameters such as the size of the firm (Mintzberg & Waters, 1982), the individual's insights, inspiration and memory, or perceived environmental factors such as external control or threats (Dean Jr. & Sharfman,

[6] Gary Stanley Becker (1930-2014) was an American economist and a professor of economics and sociology at the University of Chicago. His significant contributions were acknowledged by the field of microeconomic analysis, which broadened its scope to encompass various human behaviors and interactions that extend beyond market-related activities. Becker was honored with the Nobel Memorial Prize in Economics in 1992.

1993). As such, these complex problems present decision-makers with challenges due to the presence of *uncertainty, ambiguity* and *risk* (Hodgkinson et al., 1999; Schwenk, 1984; Tversky & Kahneman, 1974; Tversky & Kahneman, 1979). Strategic decisions may also be *time pressured*, *emotionally charged*, and *extremely consequential* (Shepherd et al., 2014). The outcomes therefore possess the potential to shape the course of the firm (Eisenhardt & Zbaracki, 1992) and exert a substantial influence on the well-being and existence of the organization (Das & Teng, 1999; Tamm et al., 2014).

Research on decision-making in intricate choice scenarios indicates that people encounter significant challenges even in making the most favorable decisions (Keane & Thorp, 2016). Furthermore, certain cognitive trails are habitually used by individuals with varying personality types, which can lead to susceptibility to biases that are present within these trails, resulting in input, output, and operational biases (Haley & Stumpf, 1989). Individuals are particularly susceptible to *framing effects* (Hodgkinson et al., 1999; Thomas & Millar, 2011; Tversky & Kahneman, 1981). Since decision-makers do not act as *"autonomous agents"* (Myburgh et al., 2015), their choices are rarely made in isolation. These decision-makers are thus contingent to *affect*, and an understanding of the *"interwoven network of issues associated with each decision"* (Langley et al., 1995). Their actions are interconnected with (i) contemporaneous decisions, (ii) decisions made by other economic actors, and (iii) decisions made over time. Strategic decisions gain greater importance when all three crucial characteristics are present (Eppler & Muntwiler, 2021). Emotions also play a fundamental role within the decision-making process and have bearing on the outcome (Druckman & McDermott, 2008; Johnson & Tversky, 1983). The existence of *information asymmetries* is another contributing factor in influencing decision-making. In such situations, individuals may attempt to justify or *rationalize* their choices. However, this is often highly subjective and thus prone to error. As such, despite good intentions, the outcome of such decision may still be poor (Kahneman et al., 2011; Trevis Certo et al., 2008). An expanding body of economic literature suggests the existence of inherent limitations in human behavior when it comes to achieving perfect rationality, even in the presence of complete and error-free information (Kianpour et al., 2021). Therefore, when elucidating the process of decision-making, it is imperative to transcend the confines of rational choice models and touch upon the realm of psychological theories (Pursiainen & Forsberg, 2021).

Essentially, strategic decisions can affect a wide variety of areas throughout the organization—including ICT and digital technology in general and cyber-security specifically. The strategic decision-making process pertaining to technology possesses the capacity to exert a significant impact on the performance of organizations, either positively or negatively. These decisions necessitate substantial resources and time for implementation and are arduous to reverse. Moreover, they are influenced by a complex array of context-dependent factors, which makes accurately estimating the prospective costs and benefits associated with such decisions challenging (Clemons & Weber, 1990). Even in the absence of a desire to leverage digital technology for competitive advantage, an organization’s executive team must still develop a strategic plan to prevent falling behind (Peppard & Ward, 2016, p. 446). Remaining inert, resembling a deer paralyzed by the presence of headlights, is not a viable option. This, in turn, places significant pressure on the company’s senior management and necessitates action in some form or another. These challenges are further compounded within the realm of digital technologies, as business problems and available technological solutions are rapidly evolving. In the past, companies predominantly viewed cyber-security as a technical matter, neglecting its broader implications (Ament, 2017; Frank, 2020). Meanwhile, it is widely accepted that the perception of cyber-security has evolved, assuming a paramount position within the context of strategic management (Gunawan et al., 2023; Maynard et al., 2018; Rothrock et al., 2018), affecting the whole organization (Hielscher et al., 2023). However, despite an increasing recognition of its strategic importance, the complete comprehension of the strategic benefits of investing in cyber-security remains elusive (Zhang, 2020). Compared to other strategic decisions in the field of digital technology, the cyber-security domain inevitably presents some unique particularities. These particularities are primarily rooted in the fact that the repercussions of any misjudgments can be severe and, in extreme cases, catastrophic, representing even existential threats to companies. Additionally, in the event of a data breach, liability issues and a multitude of legal consequences typically come into play including criminal investigations. All this underscores the significance and magnitude of the situation. As a result, decision-makers are confronted with a myriad of challenges, marked on one hand by the intrinsic complexity of strategic decisions as such, and on the other hand, due to the subconscious cognitive processes that inevitably exert influence on the decision-making process.

In conclusion, cyber-security decisions are often strategic and must be made carefully due to their significant impact on an organization’s future. These choices arise in uncertain, urgent environments and are influenced by emotions. Their effects extend beyond immediate outcomes to long-term sustainability, making it essential to understand the cognitive biases and complexities involved for effective cyber-security strategies. The subsequent subchapters will provide a more detailed explanation of the various types of cognitive impairments that exert an impact during these processes and ultimately result in erroneous decision-making.

2.4 Moral Hazard and Adverse Selection

The selection and implementation of digital technology is limited for organizations due to various constraints. A few providers dominate numerous domains, which further restricts the choices available to organizations (Carr, 2003; Moore, 2010). Furthermore, the technology space is characterized by *information asymmetries* with users having limited knowledge about product capabilities or possible bugs or flaws in a line of code deeply embedded into a given product. Such *information asymmetries* give the genesis for further effects such as *moral hazard* or *adverse selection*. For example, the proficiency required by developers to produce code that is reasonably secure is frequently confined to a relatively restricted cohort. The imposition of higher security standards results in an increase in the expenses associated with product development. In the absence of incentives, technology firms opt not to allocate resources towards enhancing their security knowledge (Vagle, 2020a). When it comes to choosing, deploying, and utilizing emerging technology, users rely heavily on a significant level of trust, sometimes even exhibiting blind faith (see Chapter 5.3). These distinctive attributes serve to magnify the *information asymmetries* between the manufacturer and the user, effectively concealing the full scope of these imbalances within an opaque system (Kianpour et al., 2021; Vagle, 2020a). In such an instance, there is an increased risk of *adverse selection*. The term refers to the presence of *asymmetric information* prior to a transaction, resulting in the less knowledgeable party opting for suboptimal products or services.[7] This disparity can also act as a catalyst for other providers to market and distribute their inferior offerings.

With the emergence of the COVID-19 pandemic and the social distancing measures imposed by governments around the world, videoconferencing systems such as Zoom, among others, went viral and triggered huge adoption rates (see e.g., Bhatt & Shiva, 2020; Nuryana et al., 2021). The remarkable expansion of Zoom has been a subject of great interest. At the pinnacle of the pandemic, the company's stock temporarily surged a staggering 450% during 2020 and was praised as "one of the 10 best stocks to buy now" (Tenebruso, 2020). Such messaging (effectively *framing*) through media and analyst coverage not only further propels the adoption rate but also serves as a mental *anchor* for attributes such as credibility, trustworthiness, quality, or success, which can trigger a *bandwagon effect* (see Chapter 2.12.2).

[7] Adverse selection can also be observed in dubious online shops, for instance. These shops tend to purchase fake reviews in order to whitewash their reputation and feign trustworthiness, which unsuspecting customers subsequently fall victim to.

All this contributes to essentially producing what may be called a “self-fulfilling prophecy”. After the initial hype, many Zoom users have been confronted with reality. Not only has the company’s share price plummeted in the post-pandemic era, meanwhile the Zoom videoconferencing software has been the subject of extensive discussion due to the numerous security vulnerabilities that were uncovered after its widespread adoption by millions of users (Kagan et al., 2020). Zoom is just one illustrative example. In general, such vulnerabilities and other software flaws are not uncommon across the technology space, and the emergence of an entire industry dedicated to cyber-security attests to the fact that it is a pervasive issue with significant legal, political, social, and economic implications (Vagle, 2020b).

In addition, *moral hazard* can manifest and have various effects. Inadequate allocation of cyber-risks ownership is a common problem, when the ones responsible for protecting the system do not face the consequences of such failures (Moore, 2010). Unfortunately, the distribution of cyber-risks is often ineffective. Consequently, any analysis of cyber-security should begin with a comprehensive assessment of the motivations and incentives of all parties involved (ibid.). In addition to the example mentioned earlier, users are not immune to the effect either. Traditionally, the insurance industry is often cited when discussing *moral hazard*. Consequently, policyholders tend to engage in riskier behavior when they do not bear the consequences of their actions themselves, but instead *externalize* the risk by shifting it onto the insurer. Similar observations can also be made in the cyber context, whereby users exhibit riskier behavior due to perceived protective measures or the implementation of cyber insurance (Böhme, 2005; Böhme & Kataria, 2006; Böhme et al., 2020). Likewise, within the realm of cyber insurance, there exists the occurrence of unfavorable risks seeking coverage to a greater extent than favorable risks (Böhme, 2005). Merely communicating about implemented security measures may already have adverse effects and tempt users (see *Nudging* and *Framing* in Chapters 2.7 and 2.12.5 respectively).

In cyberspace, the misconduct of an individual user can rapidly spread to the general population. Due to the growing interconnectivity, adverse effects are no longer limited to the own organization. The spread of ransomware campaigns such as WannaCry or NotPetya are two prominent examples having caused wide-ranging damages (see Chapters 4.2.1 and 4.2.2 respectively). When the public is left to bear the costs of such vulnerabilities, these flaws become *negative externalities* (Moore, 2010; Vagle, 2020b).

2.5 Bounded Rationality

Individuals are compelled to make decisions across a diverse range of circumstances, yet their behavior is never entirely rational, with several factors contributing to this phenomenon. However, in traditional economics, particularly in classical and neoclassical schools of thought, rationality was deemed a *conditio sine qua non*. Against this background, the social scientist Herbert A. Simon formulated a decision-making concept in the mid-20th century that is grounded in the notion of *bounded rationality*.[8] This theory posits that both internal and external factors constrain individuals' cognitive capacities, thereby limiting their ability to make fully rational decisions. More specifically, he argued that *"recent developments in economics, and particularly in the theory of the business firm, have raised great doubts as to whether this schematized model of economic man provides a sustainable foundation on which to erect a theory – whether it be a theory of how firms do behave, or how they 'should' rationally behave"* (Simon, 1955). He went on and concluded that *"there is a complete lack of evidence that, in actual human choice situations of any complexity, these computations can be, or are in fact, performed."* (ibid.). Simon's work must be seen as a major contribution to the field of economics. Based upon his accomplishments, Simon received the Nobel Memorial Prize in Economic Sciences in 1978. Meanwhile, bounded rationality has been widely adopted and *"fruitfully explored by economists"* (Shleifer, 2012). Other major contributions centered around bounded rationality originate in the field of psychology from Gerd Gigerenzer who roots his work back to Simon.[9]

Bounded rationality is an important aspect of decision-making within the cyber-security domain. The core responsibility of supervisory functions is to oversee and regulate processes, guarantee adherence to regulations, and establish control measures. Nonetheless, the element of unpredictability or the influence of human agents is frequently disregarded. Despite this, empirical studies indicate that a considerable proportion of cyber-security vulnerabilities and operational hazards can be traced back to cognitive fallacies (Bone, 2021). The cognitive limitations of humans in terms of perception and information storage are compounded by the demands and complexities of cyber-security (Pfleeger & Caputo, 2012). This is, for example,

[8] Herbert Alexander Simon (1916-2001) was an American social scientist whose work also influenced the fields of computer science, economics, and cognitive psychology. He served as a professor at the Illinois Institute of Technology in Chicago and the Carnegie-Mellon University in Pittsburgh.

[9] Gerd Gigerenzer is a German psychologist and Director of the Max Planck Institute for Human Development. He served as Professor of Psychology at the Universities of Salzburg, Chicago, and Virgina.

evidenced by the common practice of password reuse, which is often driven by the desire for convenience and self-efficacy (see *satisficing*). According to a survey, 25% of the participants confirmed compromising the security of their passwords by consciously opting for less secure options, driven by the ease of recalling simpler passwords instead of more intricate alternatives (Olmstead & Smith, 2017a). In their actions, users tend to opt for the most effortless option available, following the path of least resistance (Moustafa et al., 2021). For all intents and purposes, decision-makers tend to focus their attention on a limited number of options that may lead to achieving their goals, rather than exploring the full range of available possibilities (Das & Teng, 1999). This can restrict the generation of alternative options during the decision-making process and impact the potential outcome (Ceric & Holland, 2019). Another challenge in the field of cyber-security is the ubiquitous presence of *information asymmetries*. IT teams are constantly flooded with numerous warning messages and alerts on a regular basis. On one hand, there are instances of false alarms, while on the other hand, there is always the lurking danger that legitimate alerts may go unnoticed or that cyber-attacks have successfully infiltrated the systems without detection. In particular, the lack of expertise in the realm of cyber-security contributes to an atmosphere of *uncertainty*, leading decision-makers to rely on preconceived notions of the cyberspace that may be flawed or inaccurate (Gomez & Villar, 2018). While a greater understanding of cyber-security can counteract that tendency and enhances the accuracy of identifying false positives, significance of knowledge diminishes when it comes to identifying whether a series of activities signals cyber-attacks (Ben-Asher & Gonzalez, 2015). Another factor that adds to the uncertainty is the presence of numerous disguised actors on the attacker’s side, whose motives remain unknown, making it unpredictable when and how they will strike. This forces organizations to always maintain a constant state of vigilance. The preservation of cyber-security is undermined by users, who pose deliberate or accidental risks. Conversely, attackers perceive cyberspace as a fertile hunting ground, actively seeking opportunities to exploit information’s confidentiality, integrity, and availability for their personal gain by utilizing a range of techniques.

These combined factors contribute to the creation of a complex and demanding environment. Furthermore, during an attack, the cognitive limitations of IT teams can also impact their ability to effectively process and prioritize information, as well as solve problems (Ceric & Holland, 2019). The capabilities, limitations, and situational awareness of decision-makers vary depending on the individual (McCormac et al., 2017). This, in turn, leads to limitations that hinder the identification of vulnerabilities and effective mitigation of cyber-risks.

2.6 Libertarian Paternalism

Libertarian paternalism posits the notion that it is both feasible and justifiable to exert influence over human decision-making processes while upholding the principle of freedom of choice within certain boundaries. The underlying premise is that individuals are better off when they exercise their own judgment without external interference. The liberal nature of libertarian paternalism is preserved if the freedom of choice for those impacted is not eradicated through the design of electoral systems (Sunstein & Thaler, 2003). In essence, individuals can still retain the capacity to make decisions, even if those decisions are influenced by previous choices. The aim is to guide individuals towards rational decisions that enhance their well-being in both the short and long term, utilizing the principles of *nudge theory* to indirectly impact their behavior. Many proponents argue that *nudge theory* is thus the optimal approach to persuade individuals and aid in decision-making. However, it is important to acknowledge that while libertarianism may prove counterproductive when individuals make choices that directly harm their well-being, paternalism can be seen as oppressive and raise moral concerns regarding the actions of a governing body. Opinions on this issue vary. For example, Hausman and Welch (2010) argue that many so-called libertarian paternalistic *nudges* do not actually impose paternalistic controls but instead rely on rational persuasion, thus challenging the notion that they are truly paternalistic.

At inception, the internet itself was conceptualized as a manifestation of libertarian ideals, promoting social autonomy and creativity. The founding fathers and early adopters of the internet perceived the cyberspace as a novel, post-national social structure that embodied libertarian principles, thereby accentuating the contrast with experiences rooted in established communication networks that were predominantly regulated by governments (Hofmann, 2010). However, the internet has meanwhile morphed and is no longer that idealistic place of “peace and harmony” that the online pioneers once envisioned. Cyberspace represents all walks of life and is subject to regulation by nation states as well as hostile activities including crime. Every functioning society needs rule setting with regards to social norms. Without some degree of governance, intervention, and enforcement, the internet would be subject to anarchism. While this might have worked in the early days when the internet was not much more than an experimental playground, it has meanwhile become the backbone of modern societies and thus needs governance, much like the terrestrial world, too. From the perspective of *libertarian paternalism* in the cyber context, organizations issue security policies and guidelines, outlining how an organization’s user is expected to behave and operate when using corporate devices. In such a case, the organization gives users leeway to maneuver and operate, and make decisions, in a predefined set of boundaries, expecting the user to adhere to these principles. However, the effectiveness of such normative policies and guidelines remains questionable. A study has found that the perceived behavioral control does not have a significant impact on user conscious care behavior (Safa et al., 2015). Even software developers, who are typically more IT literate than the average user, tend to disregard or misinterpret security policies because they are often difficult to read (Balebako & Cranor, 2014). Noncompliance with cyber-security policies can be attributed to certain personality traits, namely impulsivity, risk-taking, and a disregard for future consequences. These traits are closely associated with individuals who exhibit a lack of consideration for the potential outcomes of their actions (Moustafa et al., 2021). To counter that tendency and ensure compliant behavior, security tools are often deployed to complement these written policies and guidelines. Still, there is no such thing as a perfect world. Both anecdotal evidence and empirical evidence showcase that for various reasons—whether intended or unintended—people do not always adhere to such principles and test or even overstep boundaries. In fact, despite over 90% of cyber-security teams running awareness programs, 69% of employees admit to deliberately bypassing their organization’s cyber-security policies (Candrick et al., 2023). This area warrants additional research, as it indicates that the current awareness programs may not be achieving their intended outcomes. Likewise, security tools are far from being perfect. While these tools detect and block many types of attacks, at the end of the day every computer system has certain limitations, weaknesses, and sometimes even loopholes, that can be exploited.

The bottom line here is not to suggest abandoning these policies and guidelines. It is important to give people boundaries, a moral compass, and to hold them accountable for their actions. Nonetheless, the combination of imperfect human behavior paired with imperfect security tools suggests that while the notion of *libertarian paternalism* has a role to play in the cyber context, it will clearly not be sufficient to mitigate cyber-risks. This observation is also supported by empirical studies with a mere 35% of Chief Information Security Officers (CISOs) reporting that compliance actually drives the desired behavior (EY, 2021).

2.7 Nudging

At its essence, *nudging* suggests the utilization of positive reinforcement to encourage influential individuals to undertake actions that optimize their well-being, all while avoiding any form of coercion. It entails persuading individuals, whether on a temporary or permanent basis, in a subtle manner, to modify the conduct of individuals and collectives, such as corporations or governmental bodies (see *Libertarian Paternalism*). *Nudging* also presupposes that individuals are not *homo economicus* and do not make decisions based solely on rationality. The term was first introduced by Thaler and Sunstein (2009) in their book *Nudge: Improving Decisions about Health, Wealth, and Happiness.* As highlighted by Shleifer (2012) in reference to Kahneman's (2011) *Dual-Systems Theory,* nudge proponents endorse policies that facilitate decision-making for individuals who rely on System 1 in complex situations, such as retirement savings, where even a well-informed System 2 may encounter difficulties. The amalgamation of *loss aversion* and thoughtless decision-making suggests that when an option is labeled as the default, it will garner significant acceptance. Consequently, default options possess considerable influence as *nudges* (Thaler & Sunstein, 2009). They may also serve as an *anchor* signaling an implicit endorsement. Critics argue that *nudging* is perceived as a form of manipulation due to its aim of guiding individuals towards a specific direction. This viewpoint is supported by the fact that *nudging* seeks to influence people's behavior. As per analysis by Gigerenzer (2015), Nudge is afflicted with "narrow logical norms" and lacks evidence that people are barely educable. Instead, he argues, people should be taught to become risk savvy.

Meanwhile, *nudging* has made its way into the cyber-security arena especially for awareness training. For instance, *nudge* messages can be used together with anchoring, which can be encouraging or discouraging in nature, addressing *loss aversion, fatigue* or *confirmation biases* (Sudeep, 2021). It can potentially serve as a significant factor in mitigating users' susceptibility to cyber-security threats by prompting them towards adopting risk-averse behaviors (Sharma et al., 2021). After conducting interviews with 19 software developers and surveying 228 others regarding their privacy and security practices, Balebako and Cranor (2014) arrived at the conclusion that insufficient attention is being paid to privacy considerations and guidelines. Consequently, they issued a call to action to "nudge" software developers towards adopting more appropriate security practices. But it is not only the software developers that need a nudge. Research by Van Bavel and Rodriguez (2016) found, that users frequently exhibit risky behavior not due to a lack of concern or awareness regarding the associated risks, but primarily because they lack knowledge about what secure behavior entails. As per their findings, prompting warning messages and providing training have proved useful. These observations are in alignment with the findings by Zimmermann and Renaud (2021) on the "hybrid nudge", which infers that a nudge is being complemented with further information. It has been demonstrated that this approach is equally, if not more, efficacious in promoting secure decision-making in certain contexts when compared to the simple nudge in isolation.

According to a survey by Hartwig and Reuter (2021) of over 1,000 participants (n = 1,012) throughout Germany, it was found that 64% of respondents viewed nudging in the realm of cyber-security as beneficial. However, several participants expressed concerns regarding potential risks, including deliberate misdirection, manipulation, and privacy concerns.

2.8 Satisficing

Introduced by Simon (1956), *satisficing* is a coinage combining *satisfy* and *suffice*. This term pertains to a decision-making strategy that strives to attain a satisfactory or adequate outcome, rather than the optimal solution. The notion of satisficing operates under the assumption of incomplete information, as the pursuit of additional information, which incurs costs, is abandoned once a predetermined level of aspiration has been attained or surpassed for a particular alternative. Simon proposed a novel perspective on rationality, which contends that rational choice theory (see Chapter 2.2) inadequately characterizes human decision-making processes and advocates for a psychologically realistic approach. This perspective, which Simon termed *bounded rationality* (see Chapter 2.5), posits that individuals are constrained by cognitive limitations and incomplete information when making decisions.

For the most part, time is precious. As a result, individuals exhibit a hesitancy towards dedicating extensive hours to thoroughly investigate each decision that necessitates resolution, leading to the emergence of pragmatism as a guiding principle. In essence, people are looking for an option that is “good enough” and that “serves the purpose” without exhausting all possibilities. As such, *satisficing* comes with the inherent risk that valid alternatives are being disregarded. This phenomenon also arises when decisions are made that lie outside the customary comfort zones or surpass the capabilities of the decision makers. Consequently, individuals tend to underestimate the intricacy of the matter at hand and attempt to devise a solution that fails to comprehensively tackle the extent of the problem. Regardless of one’s personal experiences, individuals are susceptible to systematic cognitive distortions, which are regarded as “errors in judgment” when examined retrospectively (Bone, 2016). From a cyber-security point of view, this constitutes risky behavior. Due to the superficiality associated with *satisficing*, there is also the risk that decision-makers will establish false connections and subsequently draw incorrect conclusions. Upon the occurrence of an event, the human psyche tends to create a narrative that provides psychological comfort by explaining the cause and potential prevention of its recurrence. This tendency to create a story by linking a series of unrelated circumstances into logical chains of cause and effect is referred to as the “narrative fallacy”. In the context of cyber-attacks, such an approach may introduce additional risks. For instance, multi-level attacks (see, for example, *Double Extortion* or *Triple Extortion*) have become increasingly common, wherein a range of attack techniques and vectors are simultaneously employed to enhance the attacker’s chances of success. Therefore, the apparent restoration or defense against a cyber-attack does not necessarily mean that the root cause has been truly addressed and the threat has been averted. It is possible that other attack techniques were concurrently utilized but went unnoticed. If a cyber-attack is only superficially examined and prematurely declared resolved, there is a real danger that the harm will continue unabated. Especially, when somebody does not comprehend the full complexity of the situation, there is the possibility that cyber-risks are being ignored and there are still gaping loopholes in the organization’s overall cyber-security posture. These flaws then typically only come to surface when it is already too late, during the *postmortem* analysis following a successful cyber-security breach.[10]

2.9 Prospect Theory

Israeli psychologists Amos Tversky and Daniel Kahneman conducted landmark research during the 1970s and 1980s that revealed consistent biases in human judgment. Their findings indicated that individuals often rely on easily recalled information rather than objective data when assessing the likelihood of a specific outcome. This cognitive phenomenon is commonly referred to as the *availability heuristic*. Additionally, Tversky and Kahneman (1979) introduced the concept of “prospect theory,” which demonstrated that decision-making is influenced by *framing* and *loss aversion*. The *framing effect* refers to the phenomenon in which decision-makers react differently to the same situation based on variations in wording, particularly positive or negative connotation. The willingness to take risks plays a central role in this process. For instance, when individuals are presented with the option of either receiving a guaranteed US$1,000 or gambling on a 50% chance of winning US$2,000 with a 50% chance of winning nothing, most individuals tend to opt for the definite gain. Conversely, when faced with the choice of either losing a guaranteed US$3,000 or taking an 80% chance of losing US$4,000 with a 20% chance of losing nothing, most individuals are inclined to take the risk of potentially losing US$4,000, hoping for the slim possibility of avoiding any loss at all. The

[10] Within IT Service Management, it is common practice to retrospectively conduct a root-cause analysis (RCA) following an incident to get to the bottom of the issue and come up with corrective measures how to prevent the reoccurrence of the problem in future. This may also be referred to as a *postmortem* analysis.

findings lead to the emergence of the “probability weighting function,” which exhibits an inverse-S shape. Further, Tversky and Kahneman (1981) denoted the term “decision frame” to introduce a cognitive framework within which a decision-maker perceives and comprehends the various actions, consequences, and potential circumstances linked to a specific choice. The adoption of a decision frame by a decision-maker is influenced by both the formulation of the problem at hand and the individual’s adherence to societal norms, habitual patterns, and personal traits.

While Amos Tversky passed away in 1996, Daniel Kahneman was honored with the Nobel Memorial Prize in Economic Sciences in 2002. In an expansion of prospect theory within the cyber domain, (Rodriguez-Priego & Bavel, 2023) conducted a study that demonstrated the greater efficacy of loss-framed messages in promoting secure behavior among participants. This finding aligns with the prevailing notion that individuals tend to respond more persuasively to negative emotions as opposed to positive ones. These findings are in line with other research in this area such as Qu et al. (2019).

2.10 Dual-System Theory

Summarizing and integrating decades of his own studies, in his book *Thinking, Fast and Slow*, Nobel Prize winner Daniel Kahneman explains the different thinking modes in the brain. Building upon Dual-Process Theory in Psychology (see e.g., Sloman, 1996; Stanovich & West, 2000), two complementary system theories are sought, both of which can form judgments or produce solutions for given decision-making problems. Depending on the situation in life and the question, people unwittingly fall back on one of the two thought patterns—one that is rule-based, intuitive and fast, and another one that is reflective, thoughtful, and slow. Of course, the human brain is not rudimentarily divided into two systems or segments. Rather, it is a gross simplification. Nevertheless, this metaphor has become established in literature and practice because it provides a framework and makes the processes in the brain more tangible (see e.g., Trevis Certo et al., 2008). The notion that associative and true reasoning constitute two distinct modes of thinking can be traced back to William James, a prominent American psychologist of the late 19th century. James expounded upon this idea in his seminal work, *Principles of Psychology* (The Decision Lab, n. d.).

In summary, according to Kahneman (2011), human cognitive processes and behavioral responses largely depend upon the intuition-based System 1. However, when faced with challenging situations, the reflective System 2 assumes control and typically dominates the decision-making. Nevertheless, as explicated by Shleifer (2012), System 2 is not infallible. Despite concerted mental effort, a considerable number of individuals would still err in solving a simple multiplication problem such as 20 × 20. While *bounded rationality* posits that individuals are prone to erroneous decision-making in complex matters, Kahneman illustrates that people even struggle in trivial matters due to their wrong approach. Nevertheless, it remains uncertain whether this pattern can be ascribed to System 1, System 2, or a combination thereof.

2.10.1 System One

System 1 operates in an automatic and expeditious manner, predominantly devoid of conscious effort and voluntary regulation (Stanovich & West, 2000). It readily provides responses to uncomplicated inquiries, often in a reflexive manner (such as determining the outcome of a basic arithmetic operation such as 5 + 5 or naming the capital city of the United States). Through System 1, individuals perceive their environment. It enables them to quickly form judgments based on incomplete and contradictory information. As posited by Kahneman (2011), System 1 remains continuously engaged and does not necessitate prior activation when confronted with a particular decision-making scenario. It elicits abilities that we have developed over time through learning and practice. According to Shleifer (2012), unlike *bounded rationality*, which involves the optimal handling of information, System 1 operates automatically and reactively, without the aim of *optimization*. However, it also tempts one to draw premature conclusions at inappropriate moments. These dysfunctions are primarily responsible for complicating accurate analyses, thus necessitating limitations on their effects.

2.10.2 System Two

The activation of System 2 occurs in response to exigent circumstances. When engaging in slow thinking, individuals exert cognitive and physical effort to systematically evaluate the information available to them. This mental exertion is accompanied by a heightened level of concentration and a sense of authority in decision-making. However, it is important to note that this process also leads to an increased level of stress. In contrast to System 1, System 2 possesses the ability to compare multiple objects, such as alternative courses of action, based on specific characteristics. Additionally, System 2 can adopt alternative perspectives when examining these objects. According to Kahneman, these two systems continuously interact with each other, with System 1 providing judgments and intuition to System 2. Thus, it can be understood as an ongoing interaction between both modes. Moreover, Kahneman et al. (2011) emphasized that when it comes to decision-making, the utilization of Systems 2 thinking can be employed by posing appropriate inquiries to mitigate the potential risks associated with encountering flaws in System 1.

2.11 Heuristics (Extract)

Heuristics are cognitive operations that help draw conclusions without having to use complicated and comparatively lengthy algorithms. It represents a cognitive generalization or rule of thumb that enables judgment and a decision to be made even with limited information, thus making it a problem-solving process which is often based on prior experiences and observations. The advantage of heuristics is that they are *efficient* since they need little attention and brainpower and lead to conclusions that are sufficient on many occasions. To that extent, heuristics subconsciously ease the decision-making in everyday situations. However, there is a risk that, predominantly in complex situations, premature and imprudent conclusions will be drawn, which are particularly undesirable when decisions of great importance are involved which are prone to judgmental errors and cognitive biases.

Amos Tversky and Daniel Kahneman have conducted groundbreaking research and a whole series of experiments spanning the 1970s and 1980s. Their findings have contributed significantly to the common understanding that heuristics per se are not inherently erroneous judgments, but rather a mechanism prone to errors in judgment. When employing heuristics, errors in judgment may or may not occur, as they are not inherently flawed but rather prone to fallibility.

These heuristics are deeply embedded into what Kahneman (2011) describes as “System One” thinking (see Dual-System Theory in Chapter 2.10). For example, in an experiment, Jalali et al. (2019) divided participants into two groups: experienced managers and non-experienced. Interestingly, the findings of their study showed no significant performance difference in the game between both groups, thereby suggesting deeply embedded heuristics in the participants’ decision-making, regardless of their level of experience. In situations characterized by dynamism and uncertainty, decision-makers exhibit suboptimal responses due to delays between their actions and the effects of their actions. The authors presume that the challenges encountered by decision-makers in such contexts are likely to be further compounded in real-world scenarios, which are characterized by a considerably more intricate cyber-security environment, featuring a greater degree of feedback delays and uncertainties. The findings illustrate the challenge organizations might face in the event of a real cyber-attack and warrant further research to improve the decision-making to achieve better outcomes.

2.11.1 Affect Heuristic

The *affect heuristic* is a cognitive bias that influences the evaluation and processing of information, and arguments based on the emotional attitude towards a situation or circumstances. Decision-makers often rely on a combination of data, knowledge, and experience when weighing risks. Whether consciously or not, our brains rely on unconscious psychological biases in the process. When a decision-maker then relies on their gut feeling, this is typically an example of *affect heuristic* (Hunziker & Fallegger, 2019). An *affect heuristic* may serve as a substitution, where the response to an easy question (How do I feel about it?) serves as the response to a much more difficult question (What do I think about it?). Preferences and aversions thus determine one’s standpoint. Following Kahneman’s (2011) *Dual Systems Theory*, these impressions, emotions, and inclinations are generated by System 1 and adopted by System 2. As a result, they manifest beliefs and attitudes, with only rare instances of verification taking place. Research suggest that these affective states and emotions significantly impact various facets of cognition and behavior (Baron, 2008) as well as the willingness to face risks (Druckman & McDermott, 2008; Johnson & Tversky, 1983). For that reason, the perceived advantages and disadvantages of a decision are primarily determined by the affective evaluation. Consequently, information and arguments that align with the emotional response are deemed more convincing, while counterarguments are often disregarded or devalued. Likewise, greater risk-taking is encouraged by anger, whereas a more cautious approach is encouraged by distress (Druckman & McDermott, 2008). As a result, decisions are predominantly based on feelings (such as fear, joy, surprise, and so on) rather than objective analysis or facts.

In the realm of cyber-security, *affect heuristics* may manifest in various ways. During the process of awarding or pre-selecting a cyber-security vendor, an *affect heuristic* may come into play. This occurs when individuals or a team from the vendor present themselves as particularly competent toward the end-user organization or when there is a great deal of personal chemistry involved (cf. Garg & Camp, 2011). Accordingly, the mood of the decision maker has an influence on the evaluation results (Schwarz, 2002). The preference or aversion towards different technologies can even influence the assessment of their costs and benefits (Kahneman, 2003; Slovic et al., 2007). However, such emotional impressions may lead to erroneous decisions. It is also possible for an emerging underdog vendor to compete against a larger and well-established player. Due to *information asymmetries*, objective abilities and performance may be overshadowed or difficult to assess for the end-user. In such cases, the more well-known player may be chosen under the pretext of avoiding mistakes and concerns about potential failures, even if this vendor does not offer the best solution under objective criteria (see also *loss aversion*). There is an unattributed, popular saying in the IT industry that *"nobody ever got fired for buying IBM,"* illustrating the dilemma that company size may serve as a trust *anchor* (see also *bandwagon effect*, *satisficing*, and *anchoring bias*). To avoid making decisions solely based on emotional impressions, it is crucial to carefully evaluate all available information before making a choice. A pre-defined set of evaluation criteria applying Systems-2 thinking may also help to achieve more objectivity (see *Dual-Systems Theory*).

In the event of a wide-ranging cyber-security incident affecting a business partner or close competitor, an *affect heuristic* may also manifest. This may lead to impulsive actions driven by anxiety, particularly if the issue has been ignored for an extended period. Panic may result in overreaction and attempts to compensate for shortcomings. However, there is a risk of overshooting the mark and incurring unnecessary costs or initiating a multitude of measures that ultimately still prove inadequate. Following the metaphor *"constant dropping wears the stone,"* it is more sensible, in the pursuit of operational excellence, to make ongoing investments and improvements toward the cyber-security posture rather than attempting to rectify past shortcomings overnight in a hasty manner. Similar observations can be made when it comes to troubleshooting. In such situations, it is challenging to maintain a calm and composed demeanor. When systems are already down and operations are interrupted, the pressure to quickly regain control over the incident is extremely high. This situation, often accompanied by feelings of loss, haste, and nervousness, is particularly prone to errors. This includes both careless mistakes made in the heat of the moment and the ability to think clearly and logically. Maintaining a calm and composed mindset in such a situation is equally important and difficult to achieve. Therefore, it is crucial for organizations to establish preparatory measures and processes that acknowledge and appreciate these circumstances, to establish a unified approach and ensure quality assurance. The *Incident Management* component from the ITIL service catalog can serve as a valuable point of reference in this regard.[11]

[11] Information Technology Infrastructure Library, or ITIL in short, represents a compilation of best practice processes and serves as the de facto standard in the field of IT service management. Organizations of all types adopt ITIL for the purpose of standardization and quality assurance when it comes to IT operations.

2.11.2 Availability Heuristics

The preference for drawing conclusions from previous events that are readily available in an individual's memory is a common phenomenon. These shortcuts, known as *availability heuristics*, are taken with *"the ease with which instances or occurrences can be brought to mind"* (Tversky & Kahneman, 1974). Events that have a lasting impact tend to be more present. However, the retrieval speed and the number of comparable incidents to be retrieved can be influenced by various factors, which are unrelated to the correct probability or frequency. Thus, relying solely on easily recalled memories can lead to poor decision-making (see also *System One* in *Dual-Systems Theory*). Utilizing memory may lead to overlooking important factors and not appreciating the specific circumstances of the question at hand. As such, there is a tendency of individuals to dramatically underestimate or overestimate the reoccurrence of events. For example, in the absence of a cyber-security incident in the preceding 12 months, a CISO might find himself in a struggle, justifying further cyber-related investments in the upcoming budget planning process. This lack of *"counterfactual thinking"* can quickly lead to problems, especially in times of economic stress or a general desire to reduce costs (Ting, 2019).

Likewise, an *availability heuristic* might also coexist with an *optimism bias*, for example when certain parts of the IT environment have not encountered any significant incident in an extended period, it may inadvertently instill a sense of complacency among IT administrators due to the infrequent occurrence of such events. Consequently, administrators may become less vigilant in implementing necessary security updates, assuming that the system's prolonged incident-free operation guarantees its continued safety (Pfleeger & Caputo, 2012). All too often, past values that are present in short-term memory are relied upon, leading to an under- or overestimation of the probability of an event. Such a distortion can also occur, for example, when a customer or competitor reports a successfully thwarted cyber-attack. This *anchor* point keeps the resilience in short-term memory omnipresent. This may also project confidence onto one's own company (see *overconfidence* and *optimism bias*), albeit little details are known about the incident due to *information asymmetries*—particularly regarding the complexity of the cyber-attack in question, the investments and safeguards implemented by the other company, the capabilities of their cyber-security team, and potentially other circumstances that played an important role in assessing the individual case. Nevertheless, this example remains ingrained in the subconscious mind (see also *representation heuristic*).

The presence of an *availability heuristic* may also impede creativity. In their study simulating a cyber-security incident, Jalali et al. (2019) concluded that inexperienced participants exhibited a significantly higher level of dynamism in their ability to adapt. Conversely, experienced managers tended to fall victim to an *availability heuristic* by replicating previous strategies. As a result, the experienced managers failed to effectively adapt and ultimately yielded subpar performance across various levels in the simulation. That said, the authors clearly stated that the results do not infer to shy away from hiring experienced managers. On the contrary, the findings of the study indicate that possessing management experience alone does not suffice in facilitating effective decision-making relative to cyber-security. It needs awareness and training to overcome these cognitive challenges.

2.11.3 Representativeness Heuristic

The utilization of the *representativeness heuristic* may result in distorted assessments of probabilities when the available information is perceived as indicative of a specific environmental trend. Consequently, the likelihood of an event occurring is either overestimated or underestimated. The greater the resemblance between an object and a particular category, the greater the probability of assigning the object to that category. Introduced by Kahneman and Tversky (1974) following a set of empirical tests, it became evident that individuals are prone to predictable and systematic errors when drawing conclusions on a sample that is not representative (see also Kahneman, 2011; Tversky & Kahneman, 1992).

From a cyber-security point of view, a *representativeness heuristic* can come to surface in numerous ways and pose unique difficulties when confronted with ambiguous information (cf. Krawczyk et al., 2013). For instance, there is a consensus among researchers and scientists that there is a significant darkfield in cybercrime (see Chapter 3.3.7 for details). Therefore, only a negligible fraction of all cyber-attacks ever makes it into the official statistics by law enforcement about reported cases. Due to the low baseline number of reported cases, it is difficult to draw any meaningful conclusions. This phenomenon is referred to as the *"insensitivity to the sample size"* (Kahneman & Tversky, 1974; Schwenk, 1984). As such, relying on publicly reported case numbers can easily lead somebody up the garden path. Reported numbers may remain unchanged for various reasons, such as victims not reporting the crime in the first place due to a lack of confidence in the justice system, embarrassment, fear of subsequent regulatory scrutiny or the crime going entirely unnoticed. This can create the impression that the cyber-threat level has not changed. Conversely, distortions can occur when better methods and advanced techniques, such as artificial intelligence-based anomaly detection, are used to detect and report more cyber-threats. Likewise, newly imposed regulations or heightened sanctions and fines for violations can balloon case numbers. In either scenario, reported numbers can suddenly surge, even though the actual underlying number of cyber-attacks have not drastically changed.

Similarly, a significant success in law enforcement, such as the busting of a criminal online marketplace in the Dark Web, where a multitude of crimes have been committed and attacks have been commissioned or criminal tools for committing crimes have been sold, can have skewing effects. While this may temporarily result in a decrease in the number of cases and cyber-attacks, caution should be exercised in interpreting these findings. The resulting gaps are known to be quickly closed. Misunderstandings and erroneous conclusions can easily be drawn from data analysis in this context. Flawed or non-representative data easily leads decision-makers to inadvertently succumb to the fallacy of identifying correlations between events that are unrelated, consequently drawing conclusions and adopting strategies that are considered ecologically irrational (Gomez & Villar, 2018). The inclusion of anecdotal information in decision-making processes (see also *availability heuristic*) has the potential to introduce bias by fostering the utilization of the *representativeness heuristic*, consequently diverting decision makers' attention from alternative sources of information (Schwenk, 1986). In practical terms, this can adversely affect strategic decision-making (Mehrabi, 2012). An incorrect assessment of the probability of a cyber-security breach gives plenty of room for inefficiencies which can have detrimental consequences, including inadequate investment or cyber-insurance coverage (Farahmand, 2018). Stanovich and West (2000) argue that even training may not eliminate the distortion but improves System 2 reasoning and the ability to recognize cues (see Chapter 2.10).

2.12 Cognitive Biases (Extract)

Cognitive biases refer to systematic errors in thinking and perception that have an impact on human decision-making. The human brain's preconceptions unconsciously influence perception, thinking, judgment, and memory. As a result, these biases appear as consistent inclinations to stray from rationality when making judgments or decisions, exhibiting a predictable pattern rather than being random. These biases are widespread and have a significant impact on strategic decision-making, especially in situations where there is a high degree of ambiguity and uncertainty (Das & Teng, 1999; Eppler & Muntwiler, 2021; Tversky & Kahneman, 1974).

Cognitive distortions occur in situations where quick action is required, when individuals are overwhelmed with excessive information, or when insufficient meaning is revealed. Memories are particularly susceptible to distortion as they are dynamically stored and retrieved, with each retrieval altering the memory itself. Despite the desire to act rationally, unconscious influences always affect an individual's decisions (Alanazi et al., 2022; Zwilling et al., 2022). The phenomenon can be attributed to behavioral patterns (*heuristics*) or distortions (*biases*). Although cognitive bias is an inherent aspect of human thinking that is difficult to prevent, not all humans are permanently biased. Some follow normative patters of rationality (Stanovich & West, 2000). In turn, a bias is contingent to the situation and circumstances (Das & Teng, 1999). The presence of numerous thinking biases does not necessarily correlate with cognitive ability. This implies that intelligence cannot accurately predict an individual's susceptibility to biases. However, research suggests that individuals with higher intelligence tend to exhibit fewer reasoning biases when provided with information on the bias and how to avoid it (Stanovich & West, 2008; Toet et al., 2016). Engaging in reflection during thinking and evaluating information is generally beneficial in identifying our own thinking errors (see *Dual-Systems Theory*).

The study of cognitive biases is a significant subfield in psychology and holds particular importance in the field of behavioral economics. The following sub chapters will provide a brief overview of some of these distortions in the cyber-security context.

2.12.1 Anchoring Bias

The *anchoring effect* is a cognitive bias whereby extraneous information serves as a fixed reference point for subsequent decision-making. This phenomenon is particularly pronounced in the context of financial markets, where it is commonly referred to as "investor bias". Introduced by Tversky and Kahneman (1974) the theory suggests that individuals, when making estimates or predictions, begin with a particular initial value or starting point (otherwise known as the *"anchor"*) and subsequently adjust from this point. The *anchoring bias* arises since these adjustments are often deficient, leading to erroneous decision-making. If, for example, in the past, a company kept the budget allocation of cyber-security expenses at a low level and no cyber-attacks were detected, this serves as an *anchor*. A newly hired or appointed CISO may face difficulties in demanding much higher expenses under such circumstances. Quite likely, internal discussions will be centered around the previous spending levels and the assumption that this was *satisficing* since no cyber-attacks have been detected. However, this completely disregards whether cyber-attacks have gone unnoticed and that the previous cyber-security expenses would prove to be significantly insufficient compared to an industry benchmark or peer group comparison.

Anchoring often coexists with *framing* and may mislead individuals to put too much emphasis on one aspect while at the same time disregarding other aspects. For example, the initial security concept or policy that a cyber-security team reviews and becomes accustomed to may serve as an *anchor*, preventing them from considering alternative and potentially superior options (see also *status quo bias*). Numbers and statistics also have a major impact and serve as *anchor* points. Especially if the estimated expenses of a service outage have been inaccurately computed (either underestimating or overestimating) and presented during a meeting as factual, it could mislead the subsequent conversation and result in unfavorable outcomes, such as inadequate or excessive investment. Given that around 33% of companies fail to assess the likelihood of cyber-risks and their consequences (see Chapter 5.1), there exists a peril where decision-makers are navigating uncharted territory. This leads to budget planning and resource allocation being conducted on flawed assumptions, resulting in *inefficiencies*.

An *anchoring bias* can also reveal their pitfalls in the context of digital technology. The impact of default options on decision making is widely recognized as one of the most firmly established effects in behavioral decision making (Dhingra et al., 2012). Even for significant decisions that would typically require careful consideration, such as selecting health care or retirement plans, individuals tend to opt for options presented as defaults more frequently than they would otherwise (Thaler & Sunstein, 2009). Software and devices are typically deployed with a certain number of preconfigured default settings. An IT administrator who encounters an insecure default setting may opt to modify it. Because of the *anchoring effect* of this initial low-level default, the alternative options, while potentially better, are still insufficient and far from the optimum (Bahreini et al., 2023). This phenomenon, where individuals tend to compare the alternative option to the default option, shares similarities with a *status quo bias* and is referred to as the *default pull* (Dhingra et al., 2012; Suri et al., 2013). Research has demonstrated that even if adjustments are subsequently made based on new data, the final estimates of values are still biased towards the initial values (Schwenk, 1984; Tversky & Kahneman, 1974). An *anchor* is so persistent that it may also lead to a biased recollection (Mathis & Steffen, 2015).

2.12.2 Bandwagon Effect

The *bandwagon effect* is a phenomenon that signifies the interdependence of demand. People change their opinion or heavily rely on the majority opinion (Dimara et al., 2018). In other words, as the market demand for a certain good increases, households tend to develop a greater appreciation for the good and subsequently increase their own demand, inferring that others want to jump onto the bandwagon, too. This effect is rooted in the inclination of households to imitate the choices made by individuals within a specific reference group. Consequently, these bandwagon effects can be perceived as a form of partial alignment of preferences.

In the technology context, a *bandwagon effect* can be observed when a certain technology is being hyped and widely featured by analysts and in the media, which thereby subtly signals to the audience “it must be good”.[12] Especially when it comes to deploying digital technologies, *network effects* come into play, suggesting that an increased *utility* of the product correlates with an increased user adoption. In essence, the greater the user community, the greater the *network externality* (Moore, 2010). This, in turn, influences decision-making and limits selection. For instance, when using videoconferencing systems or cloud services, high added value is generated through seamless interaction, shared use, and collaboration on content with others. Ultimately, the trend toward “de facto standards” narrows down the options for tool selection and fuels the *bandwagon effect*.

The creation of “monocultures” in the realm of digital technologies, referring metaphorically to the strong concentration on a few dominant providers with significant market power, gives rise to *systemic risks* (see Chapter 5.4). This applies both in the context of using cloud services (see also Chapters 5.3.4 and 5.5.4) and, at least equally importantly, for the utilization of market-leading cyber-security solutions. The letter is often underestimated. If these tools are infiltrated by an attacker through a vulnerability in the security architecture, it can result in a widespread impact. To counteract this and mitigate risks, diversifying the employed technologies is worthwhile. Study findings by Marsh/Microsoft (2018) demonstrate that these are possible means to achieve risk reduction (see Chapter 5.3.4 for details).

With the emergence of the COVID-19 pandemic, many organizations jumped toward collaboration tools including videoconferencing systems and cloud computing technology, which triggered a chain reaction and lead to skyrocketing adoption. In all fairness, in many instances organizations hardly had much of a choice because they had to ensure *business continuity* and were forced to “jump on the bandwagon” to keep their organization afloat. However, when emerging technology is hyped and acquired by early adopters, chances are that the technology is premature and prone to bugs or security flaws. The same holds true when it

[12] Certainly, less relevant from a business-to-business perspective, but consumers are potentially prone to the *bandwagon effect* too through social commerce and the work carried out by social media influencers which *“nudge”* people into one or the other direction by acting as endorsers or brand ambassadors and thereby give the company or product in question credibility.

comes to prototypes or beta versions. This, in turn, can increase an organization's risk exposure and cause unwanted consequences (see also Chapters 2.4 concerning the hype around Zoom as well as 5.3 concerning the general risk of digital technologies).

Quite concerning is that, according to research by EY, more than eight in 10 cyber-leaders (81%) have reported that their respective organizations have been compelled to circumvent established cyber-security protocols in response to the COVID-19 pandemic.

2.12.3 Dunning Kruger Effect

The *Dunning Kruger effec*t is a cognitive distortion that arises in individuals who are ignorant or incompetent in a particular area. This phenomenon leads to a significant overestimation of one's own abilities, accompanied by a deliberate disregard for one's actual competence. A manifestation of this characteristic can also be revealed by excessively simplifying a given situation. Ultimately, this is an expression of one's own inability to recognize the extent and consequences resulting from the decision. Those who do not possess knowledge are equally incapable of identifying boundaries or mistakes. Furthermore, people often disregard advice from others due to their mistaken belief of already knowing everything. The effect is named after the American psychologists, David Dunning and Justin Kruger, who conducted an experiment on this topic at Cornell University in 1999. The findings revealed that ignorant and incompetent individuals tend to overvalue their abilities, resulting in a gross overestimation of their own capabilities (see also *overconfidence bias*). A closely related observation is *naive cynicism*, whereby individuals tend to perceive themselves as less biased than their peers (Kruger & Gilovich, 1999). Persistent is the misconception that by enhancing oneself, one becomes strong. In contrast to an impostor who intentionally portrays themselves in an overly positive and impressive manner, the person experiencing the *Dunning Kruger effect* is under the false belief that they possess exceptional skills, talent, or knowledge. Narcissism can also be a contributing factor of such misconduct.

Especially in the cyber domain, such negligent behavior can expose an organization's cyber-risk exposure and become a costly undertaking if something goes wrong. Solving cyber-security problems is not a task that can be accomplished by individuals working in isolation. It is a team effort that requires the ability to recognize and successfully defend against threats. There is no place for alpha personalities who believe they have all the answers. Das and Teng (1999) found that individuals showcase an illusion of manageability and control, leading them to disregard the inherent risks associated with their decision-making. These decision-makers hold the belief that they possess the bandwidth to rectify and exert control over any potential issues that may arise. However, this illusion of control can significantly distort decision makers' ability to accurately evaluate and assess the level of risk involved (Ceric & Holland, 2019). Rhee et al. (2005) showed that such a behavior induces individuals to harbor the belief that they possess the ability to manage cyber-security threats, thereby diminishing their perception of susceptibility to cyber-attacks. Further difficulties can arise, when superiors demonstrate resistance to knowledge and do not take advice and warnings seriously, or when they fail to fully utilize the expertise of the team and instead mistakenly believe that they already possess the highest level of competence. Study results reveal additional complications caused by underestimating the rapid technological advancements and the lack of awareness regarding one's outdated knowledge (Gibbs et al., 2017). All of this can, as a result, lead individuals to underestimate the level of risk involved and overestimate their own performance, leading them to make excessively risky decisions.

2.12.4 Fatigue Bias

Every day, individuals are faced with numerous decisions to make. Each decision-making process involves a certain amount of energy expenditure, as individuals weigh the advantages and disadvantages of each option. The level of energy required for decision-making increases with the complexity of the decision at hand. As a result, individuals may experience fatigue and a decline in concentration throughout the day, leading to a noticeable decrease in productivity. Scholars in the fields of psychology and economics have identified this phenomenon as *decision fatigue*, which is characterized by a decline in decision-making abilities over an extended period.

Distraction imposes a cognitive burden on individuals. In the cyber-security context, a fatigue bias is a major risk factor. On the back of the trend toward remote working and hybrid working, a recent study concluded that a greater proportion of individuals have been found to commit errors that jeopardize the security of their respective organizations due to distractions at home. The mistakes made, among other things, include succumbing to phishing scams or erroneously transmitting sensitive information to unintended recipients (Hancock, 2022). CISOs must take the associated risks into account, especially because nearly half (48%) of respondents in a global security study carried out by Ernst & Young desired even more investments into technology to embrace remote working (EY, 2021).

Further, in a separate study most of the workforce, comprising 51% of employees, reported committing errors in their professional duties due to fatigue, which marks a 19% increase compared to 43% reporting fatigue-caused errors in the prior year. Similarly, a significant proportion of 50% acknowledged making mistakes at work when their attention is diverted, representing a rise from the 41% reported the year before. Furthermore, an equal percentage of individuals, 50%, admitted to committing errors when experiencing stress, while 34% are prone to error when they feel burned out (ibid.). At a blink of an eye, such mistakes can also have a bearing on an organization's cyber-risk exposure. Whether by clicking on the wrong link and accessing a compromised website, downloading, or opening a malicious file or attachment, accidentally sending highly confidential information to the wrong recipient, or misconfiguration, such examples abound. What all of them have in common: it does not take much to wreak havoc. In fact, research shows a direct relationship between work overload and higher job stress, which in turn impedes productivity and worsens cyber-security behavior (Hong et al., 2023).

A separate aspect of *fatigue bias* is related to cyber-security personnel, which find themselves flooded with an onslaught of security alerts daily. So-called security information and event management (SIEM) systems are designed to help IT staff systematically assess and identify legitimate alerts. However, as simple as it may sound, it is often a struggle. Depending on the source, anywhere between 25-50% of all security alarms turn out to be *false positives* causing the average organization to waste a considerable amount of time, ranging from 286 hours to 424 hours per week (Chickowski, 2019). Nearly half (49%) of organizations see this inefficiency as a major challenge (ibid.). Another exacerbating factor is the widely cited talent shortage across the IT space, and within the cyber-security domain specifically. In one recent study, 58% of all participants reported that their IT team is understaffed (Hancock, 2022). These findings are largely consistent with other studies who drew similar conclusions. In a separate piece of research, 62% of respondents said they had a cyber-security talent shortage. Just a little north of one third responded that they were adequately staffed (IBM/Ponemon Institute, 2022).

It is widely acknowledged in academic discourse that the occurrence of false alarms is perceived to foster a sense of complacency among individuals, subsequently diminishing their inclination to react to forthcoming alerts (Barnes et al., 2007; Rosoff et al., 2013; Simpson & Lyndon, 2019). The combination of end-users suffering *fatigue bias*, being stressed out and making mistakes, paired with IT teams which are understaffed, and alert fatigue is a recipe for failure and thus of great concern. Especially IT teams run the risk of encountering *false negatives*, that is that because they are flooded with false alerts and understaffed, they run the risk of not detecting a legitimate security warning and failing to respond in a defining moment.

2.12.5 Framing Bias

Framing corresponds to the use of different formulations of a message. The content of the reactions is systematically influenced by the manner in which the questions are presented, with the utilization of a reference point being a crucial factor (Thaler, 1999; Wright & Goodwin, 2002). *Framing bias* occurs when people decide based on the way the information is presented, rather than solely on the facts themselves. The *framing bias* plays a central role in the *prospect theory* of Tversky and Kahneman (1979) and is closely intertwined with other distortions. It is important to keep in mind that a problem can be presented in various manners by incorporating data or arguments to align with its *framing* in numerous situations (Bone, 2016; Gigerenzer, 2015). Recipients are inclined toward *loss aversion* (the glass is half full vs. half empty) with a predictable alteration in preference when a given problem is presented with negative or positive connotation (Hodgkinson et al., 1999; Mathis & Steffen, 2015; Tversky & Kahneman, 1981). The selection made by individuals may then differ based on the phrasing of the problem (Sunstein & Thaler, 2003), which makes *framing* one of the most influential factors impacting human decision-making (Thomas & Millar, 2011).

The use of an *availability heuristic* can often be observed too, that is, information is processed intuitively and quickly using shortcuts (see also System 1 in the *Dual-System Theory*). The effect is therefore widely used as a persuasion technique in marketing, politics, business, and other forms of communication. One of the ways to protect oneself against *framing bias* is to continually question the framing, for example by rephrasing the information and checking whether and what impact this has on the conclusion.

The reliance of preferences on the formulation of decision problems is a noteworthy concern for the *rational choice theory*. Despite the frequent utilization of message framing by cyber-security experts, they encounter difficulties in effectively communicating the desired message (de Bruijn & Janssen, 2017). For example, a major obstacle lies in the fact that discussions surrounding cyber-security and cyber-risks frequently revolve around technological aspects. Particularly when it pertains to presenting arguments to senior management, there might be a declining inclination to deeply involve themselves in the subject matter. Instead, the impression quickly arises that the issue could be delegated to subject matter experts and should be solved solely from a technical perspective. This is a misconception. Another issue to make well-informed decisions arises due to the lack of comprehensive statistics on the magnitude and extent of cybercrime, despite the growing prevalence of such criminal activities (Levi, 2017; Mehta, 2019). For example, if a company’s IT department reports an overall decrease in cyber-attacks over a specific period and shares this information with upper management, it may be interpreted as positive news. However, relying solely on the number of reported cyber-attacks can be highly misleading. With the increasing sophistication and complexity of attack techniques, it is possible that the detection rates have decreased. Nonetheless, highlighting such statistics can significantly influence the direction and outcome of discussions on this matter. Furthermore, if these attack techniques have evolved, they are not only much harder to defend, but they could also have already infiltrated the existing detection and defense systems, potentially going unnoticed. According to study findings, on average, it takes a whopping 277 days for a data breach to be detected (IBM/Ponemon Institute, 2022). Over a period of more than nine months, attackers can freely navigate through the company network, potentially spying on and extracting confidential data, without anyone noticing. It should be denoted that these are average values, meaning that there are cases where even more time elapses, allowing for a longer dwelling period to capture additional data and cause more damage. The consideration of attack numbers does not consider any of these factors. Therefore, in a hypothetical scenario where the number of cyber-attacks wane in the subsequent months following a successful infiltration of security mechanisms, and this is also reported, it holds little significance. On the contrary, it has been proven to lead to erroneous conclusions. This example highlights the interplay of various biases, such as the *anchoring effect* of the core message (“decrease in cyber-attacks”), the influence of *framing* on the conversation dynamics, the *representation bias* of potentially inadequate data, and the *optimism bias* leading to underestimation of the threat and *overconfidence* in assessing defense capabilities. Here too, it is important to mention that the insights and realizations often come to light only in retrospect, and one tends to remorsefully learn from a damaging incident rather than proactively undertaking every effort to avoid such a scenario in the first place.

2.12.6 Loss-Aversion Bias

Loss aversion states that due to cognitive biases losses tend to be weighted more heavily than gains of the same value. For example, the perceived pain of losing US$100 is often far greater than the joy of winning the same amount (Thaler, 1999). In fact, losses have a 2.25 greater impact on individuals than equivalent gains (Tversky & Kahneman, 1992). Similarly, research in psychology found that both victories and defeats cause different emotions. According to *decision affect theory*, people feel greater enjoyment when a substantial defeat has been successfully averted (Mellers et al., 1999).

Loss aversion is a central component of the *prospect theory* (see Chapter 2.9) by Tversky and Kahneman (1979). The propensity to avoid losses differs among different demographic groups, highlighting the variation in risk tolerance and decision-making patterns Cultural factors have been found to have an impact on the extent of loss aversion experienced by individuals. Wang et al. (2017) have shown that traits such as individualism, power distance, and masculinity tend to amplify *loss aversion*, while the correlation between loss aversion and macroeconomic variables appears to be relatively weaker in comparison. However, *loss aversion* can take on different forms. For example, the difference in value between winnings of 100 and 200 is perceived as subjectively greater than between 1,000 and 1,100. The same applies to the loss area. This observation is also referred to as *mental accounting*. *Loss aversion* can lead to serious mistakes with long-term negative effects in the stock market, as many investors find it difficult to realize a loss when selling a stock for less than the price at which they bought it (this may also be referred to as *sunk cost effect*). It can manifest itself in both risk-free and risky decision-making scenarios (Gächter et al., 2022). *Loss aversion* can also create an overwhelming sense of fear regarding the possibility of making an incorrect choice, leading individuals to refrain from making any decision at all (Thaler & Sunstein, 2009).

Loss aversion and fear are arguably the main reasons why people invest into cyber-security in the first place. Conversely, without having anything to lose, individuals have little incentive to make cyber-security investments (Pratama & Firmansyah, 2021). Further, research suggests a positive correlation between the cyber-threat level and human behavior. Rosoff et al. (2013) observed that following a near-miss encounter in a cyber simulation, participants demonstrated a heightened inclination to recommend a safer course of action to their companions, particularly when they were exposed to the gain-oriented message. They effectively *nudged* their counterparts and provided a new *anchor* as a point of reference.

From a cyber-security perspective, a 2022 study found that almost a quarter of all respondents (21%) said they lost their job for having accidentally send business e-mails to the wrong recipients (Hancock, 2022). However, due to a lack of incentives and possibly fear, this causes a *principal-agent conflict* and apparently leads to *loss aversion* expressed by the fact that people tend to cover-up. In the same study, another 21% of participants stated that they simply decided not to report their mistakes to the IT department (ibid.). The absence of reporting may lure the organization's leadership into a false sense of security (*optimism bias* and *overconfidence*), not knowing that because of misaligned goals and the absence of incentives, they are sitting on a ticking time bomb due to numerous security violations that have already taken place in the shadows. Harsh internal sanctions can quickly prove to be extremely detrimental and ineffective—especially if the event in question is a result of negligence rather than intent. Mistakes can occur at any given moment, as this is simply a part of the reality of life. Yet, the longer the time that elapses after a cyber-security incident or data breach until detection, the more data can circulate uncontrollably and potentially exacerbate the damage. However, research shows that *loss aversion* and *principle-agent conflicts* are not limited to employees, but also affect their superiors. Hajizada and Moore (2023) propose that there are "substantial gaps" in the regulatory filings of U.S.-listed companies, leading to incomplete disclosure of cyber-risks. This observation is consistent with other findings, suggesting that executives tend to downplay cyber-security incidents and only reveal them when investors already harbor suspicions of a 40% likelihood of an attack (Amir et al., 2018). However, it is surprising to note that non-disclosure incidents are more common than anticipated, as demonstrated by the breaches suffered by health insurer Anthem and ride-sharing company Uber. These incidents resulted in the exposure of PII data of 79 million patients and 57 million individuals respectively, leading to significant financial damages of US$115 million and US$148 million (Wong, 2017). If the cyber-security incident eventually becomes public, both the company's reputation damage and the potential sanctions (regulatory fines, compensation claims, legal fees) become significantly more costly. Therefore, organizations should work in the opposite direction and create incentives to promptly report such incidents instead of inducing cover-ups due to *loss aversion* by the affected individuals.

2.12.7 Optimism Bias

The phenomenon of *optimism bias* pertains to a behavioral tendency among individuals to overestimate the likelihood of positive outcomes and underestimate the likelihood of negative outcomes in their personal future. This cognitive distortion is pervasive in everyday life and is often observed in decision-making processes. Individuals frequently exhibit unrealistic optimism by overestimating their capacity to forecast events or their ability to exert influence over them, or by underestimating the challenges associated with realizing their objectives. This tendency can result in suboptimal economic decisions, such as those made in the context of product launches, company formation, or capital markets. According to Kahneman (2011, p. 255), optimism bias *"may well be the most significant of the cognitive biases."*

Cyber-security is characterized by *information asymmetries*. Just because a cyber-security incident did not occur in the past does not infer that such an event is not going to occur in the (near) future. Even worse: Such an event might have already happened but simply occurred unnoticed. Adversaries have the upper hand and decide *when*, *where*, and *how* to strike. They can choose from a diverse range of strategies, while defenders are obligated to meticulously examine every facet and maintain constant vigilance against any potential threat. Research indicates that people tend to succumb to the *optimism bias* and tend to assume that they are less susceptible to negative events, which is commonly known as “wishful thinking”. As a result, numerous employees mistakenly believe that they function within a secure and protected environment (Ament, 2017). Hewitt and White (2022) found that, despite possessing knowledge and lacking cyber-security protection, individuals exhibit a tendency to engage in more risky online behaviors as they underestimate the occurrence of negative effects. This also underlined by the fact that following security awareness trainings, users still only deploy basic levels of protection (Zwilling et al., 2022).

The introduction of measures to ensure information security may result in unintentional stress related to security among employees. This stress can arise when the measures are perceived as complicated and difficult to comprehend (Ament & Haag, 2016). To address this issue, security measures may be lowered to make them more understandable or to gain greater approval for the measures taken. However, this can also lead to overconfidence, as the measures may become more understandable but, when benchmarked, still inadequate. Another major consequence resulting from overconfidence in the cyber-security domain is the risk of under investments. In the absence of a cyber-security incident, managers might be inclined not to increase their budgets despite an overall surge of cybercrime, or even worse consider cutting their spending after not having encountered (or noticed) a cyber-attack. The constant arm-wrestling between the Chief Information Security Officer (CISO) and the Chief Financial Officer (CFO) about budget allocation is a typical example. IT expenditure in general is frequently perceived as a susceptible objective for cost reduction (Peppard & Ward, 2016, p. 451). Especially in times of economic uncertainty or with the outlook of an economic downtime, CFOs are strongly inclined to make the cuts (James & Kim, 2023). For instance, having polled over 1,000 cyber-security leaders, research by accounting firm EY revealed that the average organization allocates a mere 0.05% of their total annual revenue towards cyber-security. Furthermore, a significant majority of 61% of respondents indicated that their cyber-security budget is encompassed within a broader corporate expense category, such as IT. Among these respondents, 19% reported that this allocation is fixed and defined in a cyclical manner. In essence, only a small fraction of organizations perceives their cyber-security budgets as a flexible and contingent expenditure associated with conducting business operations (EY, 2021). Further, a significant proportion of respondents in the EY study, specifically 39%, express concern that their organization’s budget falls short of the necessary resources to effectively address the emerging challenges. Moreover, an additional 36% of participants concur that it is merely a matter of time before their organization experiences a cyber-security incident that could have been prevented through appropriate investment (ibid.).

The findings suggest that cyber-security is still taken too lightly and illustrates the existence of an *optimism bias* with many boards assuming "it is not going to hit us". Also, the lack of flexibility in budget allocation already assumes planning and some degree of predictability, which cyber-security incidents simply do not have. The expressed rigidity inhibits the organization's ability to react quickly and dynamically to cyber-threats and damaging events.

2.12.8 Overconfidence Bias

Typically, *overconfidence* occurs in three primary manifestations: (i) overestimation of one's own abilities, (ii) overplacement of one's performance relative to others, and (iii) overprecision in one's beliefs (Moore & Healy, 2008). Particularly individuals with low self-esteem may exhibit a tendency to overestimate themselves as a means of diverting attention from their weaknesses and lack of knowledge. Such individuals often lack self-criticality. An overestimation of one's own speed, attractiveness, performance, or intelligence can lead to a distorted assessment of the required resources and control over the situation. This allows for the differentiation of several subtypes of overestimation, such as self-enhancement, illusion of control, planning errors, and excessive optimism (Neckermann, 2020). Empirical evidence supports the significant role of overconfidence in individuals' assessments, heuristics, and decision-making processes (see also *Dunning Kruger effect*).

The impact of *overconfidence bias* is significant in real-world scenarios, particularly when it comes to professional and expert decision-making (Ferretti et al., 2016). In the field of cyber-security, this can be very problematic. Cyber-security experts are tasked with protecting sensitive information and critical infrastructure from cyber-attacks. However, if these experts are overconfident in their abilities, they may underestimate the risks and fail to take appropriate precautions. For example, most cyber-security incidents including data breaches are frequently associated with human factors, specifically miscalculations, indicating that they contribute to more than 80% of such occurrences (Soltanmohammadi et al., 2013). Moreover, overconfidence bias can also lead to complacency and a false sense of security. Cyber-security experts may believe that they have everything under control and fail to anticipate new threats or vulnerabilities. This can leave them vulnerable to attacks that they did not see coming and may result in significant damage. For example, in a recent CEO survey, 60% of respondents stated that they engage in common cyber-resilience practices (Dal Cin et al., 2023). Despite the widespread belief among numerous individuals that they are implementing sufficient safety measures against cyber-threats, this inaccurate perception of security can make them susceptible to attacks. Although following conventional cyber-resilience practices is crucial, relying solely on them is not sufficient. It is imperative to adopt supplementary measures to guarantee that both individuals and organizations are sufficiently shielded against the constantly evolving cyber-threat landscape (ibid.). What is most surprising is that 40% of the respondents did not report engaging in these practices. This observation could potentially indicate the presence of an *overconfidence bias*, whereby their own defensive capabilities are overestimated while simultaneously underestimating the likelihood of a dangerous cyber-security incident occurring (Ament & Jaeger, 2017). Further, research has observed a tendency of individuals to assign a higher value to their proficiency in cyber-security regulations or their comprehension of the security protocols and procedures that are usually implemented in such scenarios (Ament, 2017). Training is commonly perceived as a straightforward approach to bolstering awareness regarding cyber-security. However, study findings indicate that this method possesses a dual nature. Despite the significant efforts made by forward-thinking organizations to educate their workforce on cyber-security aspects, research shows that higher levels of perceived knowledge positively correlates with the misconception to be less vulnerable to cybercrime, leading to a false sense of control and riskier online behavior (De Kimpe et al., 2022; Rhee et al., 2012). Specifically, the more individuals are aware of cyber-threats and the more they feel protected, the greater the illusion of control (Rhee et al., 2005; Wash & Rader, 2015; Zwilling et al., 2022).

Similarly, studies have shown a considerable number of employees tend to exhibit overconfidence in their capacity to prevent security breaches and incidents (Frank, 2020). This ultimately resulted in a positive correlation between the level of security training and the occurrence of cyber-security incidents (White, 2015). With increasing training, individuals encountered more cyber-attacks suggesting that this was caused by the ability to better recognize events, more exposure to threats due more online usage, and more willingness to take risks. These findings align with previous research, indicating that individuals who possess information about a prior catastrophic near-miss incident such as a natural disasters or terrorist attack, devoid of any adverse consequences, are more prone to abstain from adopting precautionary measures when compared to those who lack information or possess information about a previous near-miss event that highlights negative aspects (Dillon & Tinsley, 2016). In the same vein, despite voicing concerns regarding cyber-security, individuals fail to demonstrate a significant level of *response-efficacy* and subsequently do not take precautionary measures to mitigate potential threats (Kostyuk & Wayne, 2020). This behavior persists even after receiving recommendations aimed at enhancing their online safety (De Kimpe et al., 2022). Likewise, Alnifie and Kim (2023) undertook a meta-analysis examining the phenomenon of *optimism bias* within the realm of cyber-security. Their findings reveal that *optimism bias* exerts a significant influence on cyber-risk exposure due to misconception, causing more complacency and less protective action. These findings are consistent with other research in this area concluding that an unrealistic perception of cyber capabilities translates into significant risk (Ament, 2017; Ament & Jaeger, 2017).

2.12.9 Status Quo Bias

When it comes to decision-making, individuals are often presented with the option to either do nothing or stick with their current or previous decision. The concept of *status quo bias* pertains to a phenomenon wherein individuals exhibit a preference for maintaining the existing state of affairs, despite the lack of logical justification (Samuelson & Zeckhauser, 1988). Many individuals hold the belief that despite the existence of a superior alternative, the potential benefits may not outweigh the discomfort, or difficulties associated with making a change. The extent of the *status quo bias* is contingent upon several factors, including the number of available choices, the level of awareness regarding these choices and their respective outcomes, as well as the clarity of preference for an alternative option. It is worth noting that the *status quo bias* frequently manifests alongside other departures from the economic rational model, commonly referred to as decision anomalies, such as the *sunk cost effect* and the *endowment effect* (Kahneman, 2011; Kahneman et al., 1991). The *sunk cost effect* pertains to the inclination of individuals to persist in a pursuit despite the present expenses surpassing the advantages, following an investment of resources such as finances, labor, or time. The *endowment effect*, on the other hand, denotes the act of relinquishing ownership or possession of an object. Thaler (1980) argues that *loss aversion* is a prime reason for causing a *status quo bias*. When assessing new products or services, individuals tend to base their evaluations on the perceived value rather than objective criteria. Additionally, they take into account the time required to evaluate alternative options and the potential losses associated with making a change, commonly referred to as *switching costs* (Kim & Kankanhalli, 2009). Consequently, unless the perceived benefits significantly outweigh the losses, individuals exhibit reluctance towards making a change.

IT teams often exhibit resistance towards change, citing the proverbs *“never change a running system”* or *“if it ain’t broke, don’t fix it”*. This is due to the familiarity of IT teams with the usage, properties, configuration, and interfaces of certain tools, as well as the stability of existing systems that coexist and interact in a coordinated manner. Research has also observed a tendency to simply use the default settings of a given tool rather than reviewing and personalizing the settings (Bahreini et al., 2023; Leon et al., 2012). While the rationale for not making changes may seem plausible at first glance, it is highly risky. Being caught in the “comfort zone” can lead to inertia, which is a dangerous undertaking from a cyber-security standpoint. The cyber-threat landscape is highly dynamic and constantly evolving, making it critical for organizations to remain agile, vigilant, and responsive. Some tools and processes implemented several years ago may no longer be adequate, and inertia only increases the cyber-risk exposure of organizations. Particularly, as attack techniques evolve or become more intelligent and complex, existing security tools—at least their configurations and respective patch levels—quickly reach their limits. As a result, there is a growing concern that cyber-attacks undermine systems and remain undetected. Unfortunately, the resulting vulnerabilities and issues only come to light after damage has already been done. Outdated security architecture, including outdated policies and processes, not only leads to greater susceptibility but also wastes valuable time in detection (otherwise known as the mean-time-to-detection or MTTD in short) and remediation (otherwise known as the mean-time-to-remediate or MTTR in short) in the event of an attack. The longer it takes to detect, contain, and combat a cyber-attack, as well as restore the affected systems, the more prolonged the operational downtime and typically the greater the economic damage.

To surmount these roadblocks and strive for operational excellence, it is essential to periodically review the organization’s cyber-security architecture and capabilities. The establishment and enforcement of tangible and objective KPIs (such as MTTD or MTTR, for instance) provides guidance in order to measure effectiveness and cyber maturity. Additionally, it is advisable to have the architecture validated by third parties, such as through security audits and/or penetration tests.

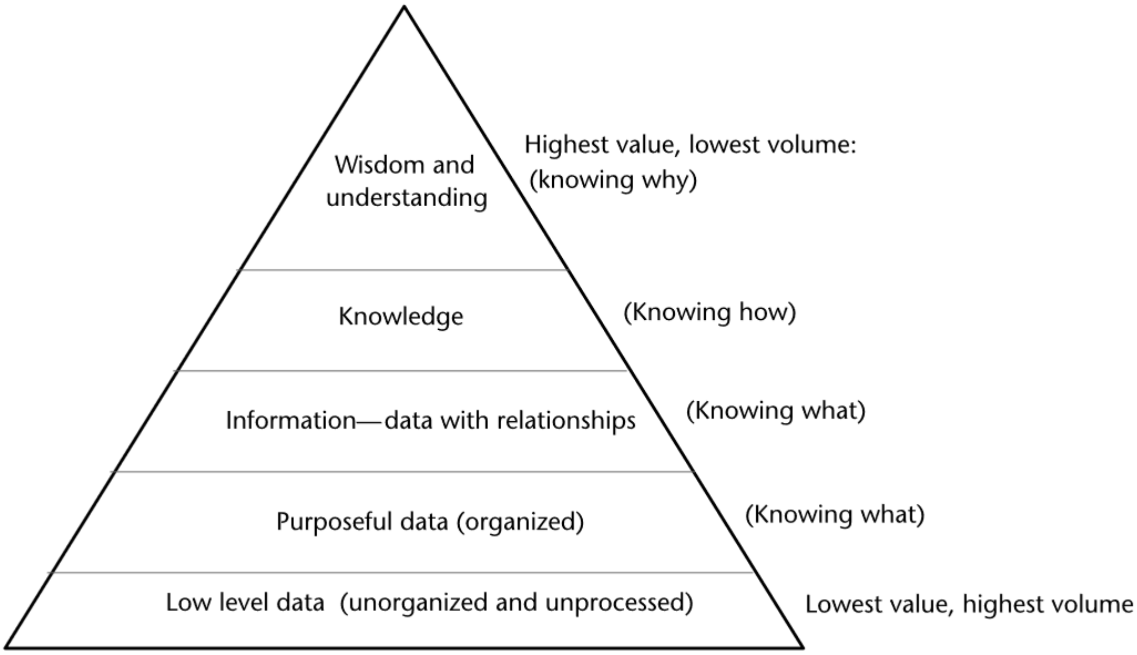
CHAPTER 3
THE CYBER REALM

3.1. Information and Communication Technology (ICT)

The importance of information and communication technologies (ICT) cannot be emphasized enough because it has become the foundation of modern society. ICT encompasses a set of technological tools and resources used to transmit, store, create, share, or exchange data and information (Weber & Kauffman, 2011). It is therefore the enabler of all kinds of digital use cases since all of them depend upon ICT.

According to Porche (2019), ICT can be imagined as a hierarchy comprising five levels of sophistication with unstructured or unprocessed data at the bottom, and wisdom at the top (see Figure 3). The illustration also indicates a negative correlation between value and quantity with the top being scarce and most precious and the bottom being largely available yet least precious.

Figure 3: The Five Spaces of ICT


Wisdom and understanding
Highest value, lowest volume: (knowing why)
Knowledge
(Knowing how)
Information—data with relationships
(Knowing what)
Purposeful data (organized)
(Knowing what)
Low level data (unorganized and unprocessed)
Lowest value, highest volume

Source: Porche (2019, p. 2)

According to Le and Hoang (2017) the cyberspace is *"all things within the realm of the ICT".* This, in turn, reinforces the importance of ICT. In other words: ICT encompasses the technical components, data, and information cyberspace depends upon.

3.2. Cyberspace

With his groundbreaking book, *Cybernetics: Or Control and Communication in the Animal and the Machine*, published in 1948, Norbert Wiener[13] is widely cited for having coined the term *cyber*, when referencing to the theoretical interaction between humankind and machines (Boyson, 2014; Ottis & Lorents, 2013). This built the basis for all neologisms such as *cyberspace*. Over time, many different definitions have evolved. Despite research spanning multiple decades, there is still inconsistency as to what the cyberspace encompasses in literature (McGregor et al., 2023; Medeiros & Goldoni, 2020; Ottis & Lorents, 2013; Strate, 1999). The following list provides an extract of the different definitions and is by no means exhaustive (see Table 2).

Table 2: List of Definitions of "Cyberspace" (Extract)

Source	Definition
Ottis and Lorents (2013)	A time-dependent set of interconnected information systems and the human users that interact with these systems.
Medeiros and Goldoni (2020)	A unique domain of artificial human interaction, disassociated in part from physical elements, which permeates the traditional domains. It exists through the connection of different layers: technological, technical, and personal. It has unique peculiarities, made possible by its partial immateriality and expansive interconnectivity. Cyberspace is constantly evolving as technology advances, and is constantly changing as different actors use it, shaping it to meet the most diverse needs.
Buckland et al. (2015)	The interdependent network of information technology infrastructures.
Li and Liu (2021)	Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval, and exploitation of information.
Strate (1999)	Cyberspace covers three levels, which are (i) ontology, which includes notions of cyberspace as a para-space or non-space, as well as the concept of cyberspacetime, (ii) building blocks such as

[13] Norbert Wiener (1894–1964) was an American mathematician and Professor at the Massachusetts Institute of Technology (MIT).

	physical conceptual and perceptual space or virtual space, and (iii) a level of synthesis, including varieties of cyberspace such as media space, aesthetic space, dataspace, and personal and social space.
Eling and Schnell (2016)	The interactive domain composed of all digital networks used to store, modify, and communicate information.
Pijpers (2023)	A constellation of computer networks within which binary data are stored, modified, and transmitted generating a virtual platform of communicative interaction. The virtual dimension represents a notional abstraction of objects, persons, occurrences, systems or realities and partially overlaps but is not synonymous with cyberspace.

Source: Author

Despite “cyberspace” being a widely used term and a cornerstone of digital transformation, the examples above illustrate that there are still lots of inconsistencies. Because of the broad nature of the term and varying definitions, this makes clarification of the scope *a priori* necessary (McGregor et al., 2023). In relation to the concept of cyberspace, the definition proposed by Eling and Schnell (2016) will be adopted for the purpose of this thesis.

3.2.1. Cyber Politics (Cyberization)

As outlined by McGregor et al. (2023), the notion of cyberspace being viewed exclusively as a technological realm is a prevalent theme in contemporary literature. Nevertheless, in recent times, the concept of cyberspace and its associated definitions have permeated a diverse range of disciplines, including but not limited to information and national security, international law and cybercrime, social-political domains, internet governance, and even cyber-geography. Indeed, both state and non-state actors are increasingly pushing the boundaries of the cyberspace to advance their political agenda and geopolitical interests (Limnéll, 2018). This transition is commonly known as *cyberization* (Kremer & Müller, 2014). Besides launching cyber-attacks, the distribution of propaganda, disinformation campaigns aimed at influencing the political discourse, and the interference of electoral processes have become a matter of concern. These malicious activities are conceptualized to erode trust and solidarity, and shape the public opinion, causing uncertainty, fear, and divide.

While Russia’s meddling in the 2016 and 2020 U.S. elections is well-known, this is only the tip of the iceberg. In 2023, the Russian FSB has been accused by the UK government of conducting cyber operations against the United Kingdom for years. These allegations follow prior claims made by the UK government, accusing Russia of interfering in the 2019 election (Corera, 2023). Similar instances have been observed across the European Union. Countries such as France, Germany, Sweden, the Netherlands, and the Baltic states have reported cases alike, highlighting the broader issue of foreign interference (Blackwill & Gordon, 2018; Brattberg & Maurer, 2018; Egloff & Smeets, 2023). The European Parliament also experienced a significant disruption through DDoS attacks in 2022, coinciding with its decision to designate Russia as a state sponsor of terrorism. A pro-Kremlin group later claimed responsibility for the attack (Meijer & Siebold, 2022). Similarly, the Belgium parliament was brought to a halt after being hit with DDoS attacks during a heated debate on the alleged genocide of Uyghur Muslims in China, with a Chinese APT group identified as the perpetrator (Sharwood, 2022). Months later, a Belgian Member of Parliament was targeted by a Chinese threat actor with a spear phishing attack after authoring a resolution on the crimes against the Uyghur minority (Yang, 2023). While Russia and China are prominent culprits, offensive cyber capabilities are being pursued by more than 30 countries worldwide (Goel, 2020). As such, *"security policy in the information age faces formidable challenges"* (Kello, 2013). Specifically, the issue of cyber-attacks representing a "gray area" within politics, warfare, and international law has frequently been raised (Radziwill, 2015). As outlined by Kello (2013), *"because cyberweapons are not overtly violent, their use is unlikely to fit the traditional criterion of interstate war; rather, the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace—with important consequences for national and international security. Although the cyber revolution has not fundamentally altered the nature of war, it nevertheless has consequences for important issues in the field of security studies, including nonmilitary foreign threats and the ability of nontraditional players to inflict economic and social harm."*

In reflection of the above, it is increasingly acknowledged that the cyberspace evolves into a strategic domain in the 21st century, which raises fundamental questions around territorial sovereignty, state monopoly, and accountability between international actors (Baldini et al., 2020; Li & Liu, 2021; Medeiros & Goldoni, 2020). This is an area meriting further analysis.

3.2.2. Deterrence and Attribution

Shahid and Khan (2022) posit that deterrence by punishment represents an alternative to the deterrence by denial concept. The former strategy operates by communicating to the adversary that the consequences of their actions will be severe. To be effective, the threat of retaliation and punishment must be perceived by the adversary as outweighing any potential benefits. Consequently, the establishment of attribution for the action is crucial for the threat of retaliation to be successful. In theory, the application of deterrence by punishment in the cyber domain follows the same principles (ibid). However, the nature of the cyberspace is still such that attribution of concrete actions to a specific actor with a high degree of confidence remains difficult (Li & Liu, 2021; Medeiros & Goldoni, 2020; Scherbina & Schlusche, 2023) and prone to error (ENISA, 2021), which undermines the idea of deterrence. Anecdotal evidence suggests that even ascribed cases hardly had any deterrent effect. For instance, Russia's attempts to undermine the 2016 United States elections and create distrust in American democracy were widely recognized in the aftermath of the event. However, the reaction from the United States was unexpectedly limited and ineffective. According to Blackwill and Gordon (2018), the Obama administration was *"slow to realize the full extent"* of the situation and only imposed a small number of retaliatory measures. Conversely, the Trump administration did even less, as President Trump himself trivialized the events by opposing any actions and urging the nation to focus on *"bigger and better things"* (McCaskill, 2016). In parallel, the U.S. Intelligence Community expressed a high level of confidence that the hostile cyber operations were *"authorized at the highest levels of the Russian Government"* (Limnéll, 2018). Despite the turmoil it caused, the gravity of the accusations, and the international media coverage, Russia faced minimal consequences for its actions. Although the FBI indicted 12 Russian military intelligence officers for their alleged involvement in election interference, it remains uncertain whether these individuals will ever be extradited and prosecuted for their actions (FBI, 2016). Making matters worse, the provocations using cyber-attacks have just continued and further intensified, with no discernible indication of a significant turning point on the horizon. The upward trajectory of cyber-attacks remains steep, with their numbers steadily rising. Regrettably, all attempts to attain a consensus among nation states how to deescalate cyber warfare has not yet materialized (Goel, 2020).

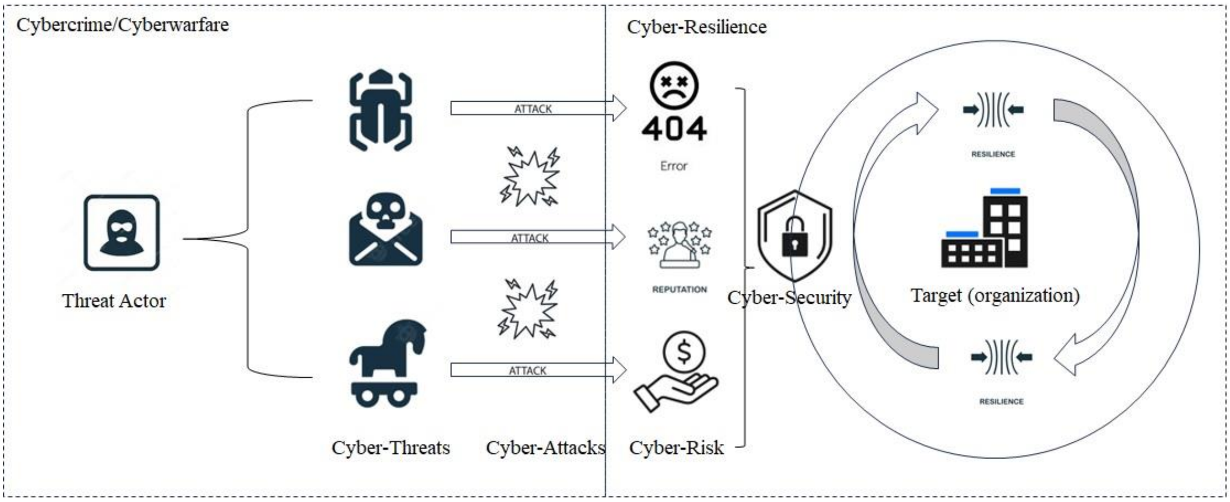
3.2.3. Lack of Norms

The complexity of cyberspace leaves immense room for speculation since threat actors can disguise their identities, intentionally leave false evidence to divert the attention and incriminate someone else. At the same time, international law is ill-equipped to handle hostilities related to cyberspace. Legal norms cannot keep up with technological advancements, resulting in a void that certain nation-states are exploiting to their advantage. The response of states to cyber-attacks will thus be contingent on the specifics of each case (Limnéll, 2018). Certain legal scholars go further and contend that a State that has been victimized may employ force as a means of self-defense against another State, provided that the attack was perpetrated by the latter's organs or agents, or by non-State actors that were tolerated by the State in question. In the absence of a state actor, the victim State may take action in self-defense against the non-State actor (Tsagourias, 2012). The manifestation of all these governing norms is still pending, leading to uncertainty, and hindering deterrence, countermeasures, and prosecution.

3.2.4. Contextualizing the Cyber Domain

Now that cyberspace has been introduced, prior to delving into the notion of cybercrime, it is worth acknowledging that the cyber domain might appear a bit overwhelming at first glance. In particular, the abundance of cyber-acronyms can be perplexing at times. Therefore, this subsection aims to provide a high-level introduction to contextualize some of the key terms, and their respective interplay within the cyberspace, that will be used and referred to in subsequent chapters (see Figure 4).

Figure 4: The Cyber Domain



Source: Author

Within cyberspace, various *threat actors* engage in malicious activities (for simplicity stake, in the aforementioned illustration, the attackers are depicted on the left, and the defenders are depicted on the right). Depending on the threat actor's motive and identity, these malicious activities are then either referred to as *cybercrime* or *cyberwarfare* (see Chapter 3.3.2 for details). *Threat actors* use different types of malicious mechanisms and techniques to accomplish their goals, which can be broadly understood as *cyber-threats*. When carrying out an attempt to strike, this is typically classified as a *cyber-attack*. These attacks in turn pose *cyber-risks* for organizations, jeopardizing reputation and potentially causing business disruption and financial damages. These end-user organizations are potential *targets* (otherwise known as victims or victim organizations). To reduce *cyber-risks* and build protection, they hire *cyber-security* experts and deploy *cyber-security* tools. The collective effort of reducing risks, deploying tools, hiring experts, and building appropriate capabilities to mitigate, contain and withstand *cyber-attacks* paired with the aptitude to quickly restore business operations following an attack is ultimately referred to as *cyber-resilience*.

3.3. Cybercrime

Cybercrime, out of all the categories of criminal activities, exhibits the most rapid growth according to Interpol (WEF, 2020). Even though cybercrime is a widely used term, there is no universal definition. Put simply, cybercrime is crime in the cyberspace (Farahbod et al., 2020) or offenses at the crossroads of cyberspace and crime (Arief et al., 2015; Singh & Bakar, 2019), encompassing any unauthorized activity involving a system, equipment, or network (Li & Liu, 2021). Built upon previous research (Goodman & Brenner, 2002; ITU, 2012; Maras, 2016; Wall, 2008; Wilson, 2008), the United Nations broadly defines cybercrime as an "*act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime"* (UNDOC, n. d.-a). Further attempts have been made by Chandra and Snowe (2020), to come up with a theory-based taxonomy for cybercrime. As per their suggestion, "c*ybercrime is an act in which the use of a computer, its related technology, and/or the networked systems within which it functions, integrally facilitates, or enables the criminal action. This definition fundamentally distinguishes the nature of cybercrime from that of a traditional criminal act (offline)*". However, cybercrime is not a new phenomenon; it has developed and, along with the adoption of ICT, exponentially gained importance over time to becoming a complex and highly organized business (Farahbod et al., 2020). As emphasized by Manky (2013), in the early days, with the computerization of phone systems, people already explored how to manipulate and exploit these systems for personal benefit, namely the reward of free calls. As computerization expanded into more facets of life, cybercrime disseminated in parallel. However, it was only in the late 1990s that the term "cybercrime" emerged.

The risk of facing a crime is not evenly distributed across a population, and normally considered to be a rare occasion (Prieto Curiel et al., 2018). Conventional crime tends to be concentrated among certain groups of people in specific geographical areas, and it fluctuates over time in waves (Freeman, 1999). This makes certain groups statistically immune against crime while others are prone to chronic victimization, suggesting that there are a funneling effects (Felson & Boivin, 2015; Prieto Curiel et al., 2018). Cybercrime, in contrast to traditional crime, has become widespread, random, and unpredictable, having the potential to impact any individual using the internet. No one is immune.

Routine activity theory (RAT) posits that individuals who are motivated to commit offenses will take advantage of opportunities when they come across vulnerable targets that are not adequately protected. RAT emphasizes the importance of three key elements: (i) motivated offenders, (ii) suitable targets, and (iii) the absence of capable guardianship (Cohen & Felson, 1979). It suggests that when these elements align, the likelihood of criminal activity increases. Although the application of RAT in the cyberspace is subject to reservations and limitations, including a restricted sample size and a narrow range of crimes under examination (e.g., Cook et al., 2023; Leukfeldt & Yar, 2016), the extent to which people use the internet and participate in activities such as focused browsing and direct communication seems to be largely correlated with their susceptibility to cybercrimes. As individuals spend more time online, they become more vulnerable to potential dangers and the likelihood of becoming a victim (Leukfeldt & Yar, 2016; Reyns et al., 2011). Partaking in particular online behavior poses greater risks than others, leading to heightened vulnerability to cybercrime (Lahcen et al., 2018). For instance, engaging in gaming, dating, and pornography websites further amplifies the risk exposure (Gainsbury et al., 2019). The presence of internet addiction plays a crucial role too in determining the probability of participating in riskier behaviors (Hadlington, 2017). Interacting extensively on social media platforms, for example, is an activity that some individuals tend to do more frequently than others, which in turn can increase the odds of moving into the crosshairs of cybercriminals (Saridakis et al., 2016). Attackers rely heavily on social engineering methods, including impersonation and phishing e-mails, as their primary strategies (Alnifie & Kim, 2023; D'Hoinne, Watts, & Thielemann, 2022). The threat in this context is tangible, as evidenced by the Uber breach that resulted in a staggering US$148 million in damages caused by a phishing attack (Wong, 2017). This incident serves as a prime illustration of how social engineering can be employed to infiltrate and organization.

Unlike regular crime, cybercrime typically comes without such geographical or physical boundaries and makes these considerations obsolete. It is a developed form of transnational crime (Maillart, 2019; Sviatun et al., 2021) which makes prosecution difficult (Moraski, 2011). One of the driving forces of crime in the cyberspace are the spatiotemporal nature of actions, unclear identities, and lack of deterrence (Karuppannan, 2009). To that end, traditional theories of crime causation should be extended. Going forward, Topalli and

Nikolovska (2020) propose that criminological theory development should more clearly discerns whether a crime has been committed *wholly*, *partially*, or *not at all* within the cyberspace. It could be contended that there is a “perfect storm”, where a convergence of multiple factors creates a golden opportunity for cybercriminals to exploit. The combination of global digitalization efforts (i.e., technological advances and productivity gains through increased usage of ICT infrastructure and networks; the establishment of data-centric business models; etc.); a broader attack surface that comes along with that leading to greater vulnerability, coupled with anonymity of the internet; low entry barriers and a perceived enforcement gap, which allows perpetrators to get away without being brought to justice, turn the cyberspace into a hunting ground for criminal activity (Li & Liu, 2021; Singh & Bakar, 2019).

3.3.1. Cybercrime in Narrow Terms vs. Broad Terms

Some authorities distinguish whether the computer is the tool or the target (Jakobi, 2013). Others differentiate between crimes targeted against IT infrastructure, networks, and data, which are purely committed online (otherwise known as *computer crime*). This is referred to as *cybercrime in narrow terms*. It contrasts with offenses committed online, that could have been carried out in the analogue world too, in which the computer was just a supporting element, such as trading drugs or firearms, for example (otherwise known as *computer-related crime*). The latter is then referred to as *cybercrime in broad terms* (BKA, n. d.).

Equally, McGuire and Dowling (2013) compartmentalize offences into *cyber-dependent crimes* and *cyber-enabled crimes* in the following way:

> *“Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e., the flooding of internet servers to take down network infrastructure or websites. [...] Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.”*

> *“Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT.”*

In the context of this thesis, *computer crime* and *computer-dependent crime* will be treated as synonymous and categorized as *cybercrime in narrow terms*. Likewise, *computer-related crime* and *cyber-enabled crimes* will be treated as synonymous too and categorized as *cybercrime in broad terms* with the latter being in scope of this work.

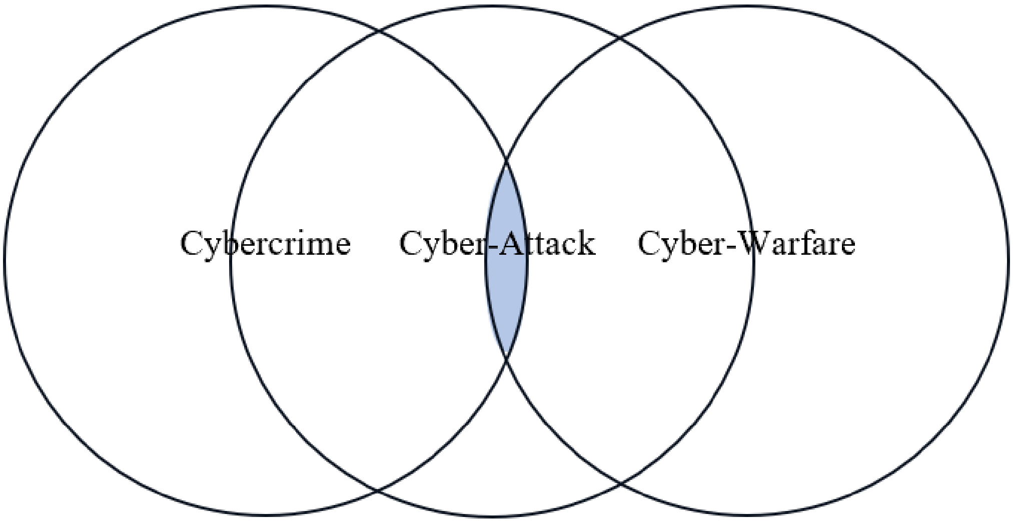
3.3.2. Cybercrime vs. Cyberwarfare

Though the terms *cybercrime* and *cyberwarfare* appear to be sometimes used interchangeably, they are not synonymous. With increasing digitization, various hostile nation states are meanwhile operating in the cybersphere as well. Unlike regular cybercrime, which is largely financially motivated, cyberwarfare is politically motivated and can only be conducted by a rogue foreign nation state. Cyberwarfare has destructive effects (Maras, 2016) and the potential to cause catastrophic damages above and beyond a regular cyber-attack. It aims to disrupt utilities and other critical infrastructure, cripple economies, and cause political unrest (Atrews, 2020). In contrast to traditional terrestrial warfare, and espionage, cyberwarfare is a fundamentally new military doctrine (Bringsjord & Licato, 2015) and the extension of offensive action and counteraction by a nation state into the digital realm (Kapto, 2013). The cyberspace provides an operating theater for hostile nation-states to advance their so-called 5D agenda, that is, *disinformation*, *deception*, *destabilization*, *disruption*, and tailored *destruction*, which are powerful instruments to exude political influence (Denić & Devetak, 2023).

Cyber conflicts exhibit distinctive attributes, as opposed to conventional military conflicts, whereby Information and Communication Technology (ICT) is weaponized instead of traditional military weaponry and armed forces. Cyberwarfare serves as a complementary domain to conventional warfare, enabling nations to surreptitiously incapacitate vital infrastructure and communication channels, without the need to secure physical territory (Chen & Dinerman, 2018). It can be seen as a "digitalized" variant of *asymmetric warfare* which aims to provide a strategic advantage to exert influence at low costs (Kim, 2022). Nobles et al. (2023) define asymmetric or asymmetrical warfare, otherwise known as asymmetric or asymmetrical threats, as *"the disproportionateness between two challengers and the strategies exercised by the weaker challenger to cause the strengths of the stronger challenger to be doubtful."*

Primarily, cybercrime and cyberwarfare exist as distinct disciplines, and threat actors can employ cyber-attacks to achieve their respective objectives. However, it is crucial to recognize that while cyber-attacks may seem like the most obvious *modus operandi,* they are not the sole option available. For example, a cybercriminal could unlawfully duplicate files onto a USB stick or enlist an insider to do so, or they could physically steal a device. These actions constitute theft rather than a cyber-attack in the true sense of the term. Similarly, copyright infringements, cyberbullying, cyberstalking, and scams are all forms of cybercrime that do not necessarily involve a cyber-attack. Instead, these malicious activities represent different types of cyber-exploitation. Likewise, cyberwarfare can take various forms, including disinformation campaigns, which do not qualify as cyber-attacks either. Therefore, while cyber-attacks are widely utilized, they are just one tool among many in the cyber-arsenal that threat actors can employ (see Figure 5).

Figure 5: Distinction between Cybercrime, Cyber-Attack, Cyber-Warfare



Source: Author

While cybercrime and cyberwarfare are typically distinct, Figure 5 highlights their notable overlap, with the North Korean government exemplifying this by conducting digital heists and plundering crypto exchanges to subsidize its weapons programs (Kim, 2022). Whereas cyber-warfare, by the various definitions, is normally not financially motivated, in case of North Korea, it is (see Chapter 4.3.7 for details). Therefore, the terms *cybercrime* and *cyberwarfare* are not mutually exclusive. However, technically speaking, the overlap is only one dimensional and not binary. *Cybercrime,* which largely encompasses cyber-operations motivated by financial gain, can be carried out either by a hostile nation state or an entity supported by the state. However, it is improbable for a cybercriminal to engage in *cyberwarfare* activities. Typically, *warfare* is associated with actions undertaken by a nation state, although there are occasional instances of unconventional warfare conducted by guerrilla or militant groups.

Publicly witnessed in the wake of Russia's war against Ukraine, a relatively new phenomenon is the concept of *Dual War*, whereby a conventional military operation with ground forces is being backed up and supported by various sophisticated cyber-operations at scale (ACSC, 2022).[14] A new "blueprint" is the trend of hacktivist groups building a coalition with state-actors or the military itself to extend the battlefield and fight the enemy in the cyberspace (SecAlliance, 2022). Though the concept of hacktivist groups working in support of military forces may be a new phenomenon, hybrid threats per se are not. NATO characterizes them as follows:

> *"Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies."* (NATO, 2023).

According to both NATO (2023) and the European Defense Agency (n. d.), aimed at destabilizing opponents, hybrid methods of warfare including propaganda, espionage, deception, sabotage, and other non-military tactics have been applied for long. What is new in the recent past are the speed, scale, and intensity of these methods, amplified by rapid technological advancement and increased global interconnectivity. Meanwhile, cyber-operations are used much like other covert operations were used during the Cold War to advance foreign policy and undermine other nation-states (Jensen, 2017). In essence, cyberwarfare is a tactic of concealment. The perpetrators try to either operate anonymously or deny involvement in incidents and conflicts. They are doing this carefully and in a coordinated and nuanced manner, without crossing the threshold into an armed attack (Egloff & Smeets, 2023; Harknett & Smeets, 2022; Maness & Valeriano, 2016). This raises the question what legal framework or democratic process govern any decision to respond (Buckland et al., 2015). However, these covert cyber-operations could be interpreted as modern day application of a what has previously

[14] For clarification purposes, the concept of *Dual War* is not to be confused with a *Two-Front War*. The first effectively suggests one kind of a *Multi-Domain Conflict* (in the aforementioned example two-dimensional, covering cyberwarfare and terrestrial warfare) against the same enemy, whereas the latter describes a conflict against two or more allied parties engaging the opponent on geographically separate fronts. While the term *Dual War* was used by the Australian Government to contextualize the conflict between Russia and Ukraine (e.g., ACSC, 2022), *Multi-Domain Conflict* or *Hybrid War* are perhaps more common terms.

been referred to as a *pin-prick policy*, that is, akin to an unconventional warfare strategy, a method that leverages subversion to undermine the enemy.[15] In this case, according to Jain (2014), the *"pin-prick doctrine permits defensive uses of force in response to a continuing pattern of attacks providing objective proof of a future threat"*. In contrast to Buckland et al. (2015), the application of a pin-prick policy, aimed to conduct counter strikes, would not only provide a framework how to respond, without having explicitly used this terms, anecdotal evidence suggest this has already been practiced, for example, when looking at the offensive actions taken by Western state actors in response to cyber-threats (see Chapter 4.3.7).

An interesting and alternative perspective provide Harknett and Smeets (2022), by minting the term *cyber-competition*, when referring to the geopolitical rivalry between nation states in the cyberspace. This view contrasts with the premise that cyber-warfare inherently has *destructive effects*. In fact, it refers to a lower threshold and *degrading effects* instead. To that end, the scale and scope of cyber activity is operationalized with an intent to achieve strategic advantage by shifting the distribution of power through continuous campaigns comprised of often-covert, less violent cyber-operations with cumulative effects.

3.3.3. Cybercrime-as-a-Service

Cybercrime has evolved from a niche market into a mass market. Following the market model of criminal offenses introduced by Ehrlich (1996), the "cybercrime market" as such *"is not necessarily a physical setting where illegitimate transactions are contracted"*. It can rather be characterized as a Walrasian[16] market in which *"the aggregate behavior of suppliers and demanders is coordinated and made mutually consistent through adjustments in relevant prices."*

Cybercrime has meanwhile turned into a sustained business and a global threat for governments and companies alike (Huang & Madnick, 2017; Nobles et al., 2023). Germany's Federal Criminal Police describes today's cybercrime as a *"professional field of business"* (BKA, n. d.). As such, there is a highly organized hierarchy involving multiple roles and functions including engineers, infantry, leaders, and hired money mules. These syndicates exhibit a fully-fledged business model and monetization strategy allowing even an illegal

[15] Overseen by an official yet highly secretive committee, the British government applied a coherent strategy of covert action during the Cold War that is referred to as the "pinprick" approach.

[16] The Walras' law was developed by Leon Walras (1834-1910) to showcase that a state of *general equilibrium* in which supply equally meets demand at the same time in all markets can exist.

company to pay their bills in order and to function on a day-to-day basis (Manky, 2013). The emergence of the Cybercrime-as-a-Service (CaaS) has been acknowledged as a *”critical evolution in the cybercrime landscape”* (Akyazi et al., 2021). CaaS remains a cornerstone of the underground economy and a profitable revenue-machine. Notably, the rise of the Dark Web has further facilitated the commodification of cybercrime.[17] Consequently, individuals lacking hacking expertise can now easily engage the services of criminals or purchase hacking tools from various underground marketplaces (Delamarter, 2016; Manky, 2013; UNDOC, 2013). There is so much commercialization that even *“less-than-prodigious hackers may choose it as a profession”* (Huang & Madnick, 2017). The prevalence of inexperienced novices among hackers on online platforms is becoming increasingly apparent, as indicated by a substantial amount of research. This can be attributed to the relatively low entry barriers that exist in this domain (Holt et al., 2012; Huang et al., 2018; Li et al., 2016). Meanwhile, more than 24 different illicit business models and service categories have been identified (Huang et al., 2018). The difficulty of profiting from stolen data had been a persistent issue for cybercriminals, but advancements in cybercrime black markets and the widespread adoption of cryptocurrencies have seemingly addressed this problem (Lewis, 2018). Various marketplaces as well as individual websites on the Dark Web serve as sales channels for hackers to monetize their skills (Denić & Devetak, 2023). These illegal marketplaces on the Dark Web, sometimes also referred to as “crypto markets” (Aldridge & Décary-Hétu, 2014; Décary-Hétu & Giommoni, 2017; Jeffray & Feakin, 2015; Martin, 2014; Ouellet et al., 2022), are where supply meets demand. As correctly pointed out by Akyazi et al. (2021), the CaaS business model would not be possible without customers demanding malicious cyber services and products.

Like legitimate e-commerce, with just a few errand clicks, cybercriminals provide their skills at fixed rates on a per-job basis and a huge variety of illegal products can be purchased, too. Bizarrely, it is not uncommon that a CaaS offering comes along with “customer support” and some kind of a helpdesk function, to ensure the customer has a positive experience and is satisfied with the ill-minded products purchased (ACSC, 2022). CaaS covers an ever-growing portfolio of data, services, and tools to utilized facilitate illegal cyber-operations (see Table 3).

[17] The Dark Web is a hidden space beneath the regular Internet. It is a logical structure primarily designed to protect user identity and network activities (Denic and Devetak, 2023). Terminology such as “Dark Web”, “DarkNet”, and “DeepWeb” and is sometimes used interchangeably, but these terms describe distinctively different technical concepts. For a taxonomy of the “hidden Internet” and detailed discussion about DarkNet, Dark Web, and DeepWeb and the differences between these terms see e.g., Weimann (2016), Hatta (2020) or Denic & Devetak (2023).

Table 3: Dark Web Price Index 2023 (Extract)

Item for Sale	Price
Various European Union passports	US$3,000
Swiss Online Banking Account	US$2,200
Polish ID card	US$1,700
2.4 million Canadian emails	US$100
50 Hacked PayPal account logins	US$120
United Arab Emirates credit card with CVV	US$35
Hacked Instagram account	US$25
German passport template	US$22
Israel hacked credit card details with CVV	US$20
U.S. eBay account	US$20
DDoS attack with 10k-50k requests per second on an unprotected website for 1 hour	US$10

Source: PrivacyAffairs (n. d.)

It is important to note that CaaS does not entirely rely on the Dark Web. Meanwhile, several CaaS services can even be found on the regular internet (Nobles et al., 2023). These services are often then hosted in jurisdictions with below-standard law enforcement capacity or loopholes in their respective criminal codes, so that the shady business model is not punishable under local law. Sometimes, corruption might be a contributing factor as well. Much like legitimate e-commerce sites on the regular internet, these underground marketplaces often resemble their appearance with "eBay-style shop frontends" (Aldridge & Décary-Hétu, 2014). In the case of physical items, the vendors engage in international shipping of their unlawful merchandise through postal services (ibid; Décary-Hétu & Giommoni, 2017; Ouellet et al., 2022). With the growing numbers of illicit underground marketplaces, there is increasing competition and commoditization, which prices certain types of cybercrime in the same ballpark as, or even below, many entertainment products (Noroozian et al., 2016).[18] For instance, while generic spamming was priced at US$13 per 10,000 e-mail messages in 2011, the price dropped to US$5 in 2014 (Kadlecová, 2015).[19] Although these price tags appear to be

[18] For a comprehensive overview of CaaS offerings and price points see e.g., Manky (2013); Akyazi et al. (2021) or Huang et al. (2017; 2018)

[19] Anecdotal evidence suggests that there has been commoditization in the overall ICT market in recent years. Due to the advent of Cloud Computing and internet broadband, economies of scale have driven the costs down, making the use of IT infrastructure, data storage and data transmission more cost effective. Further research is

tiny in the greater scheme of things, trade can still be very profitable. Case in point, following the Yahoo data breach in 2013 which exposed a total of 3 billion e-mail addresses, even years later all these e-mail addresses can still be purchased on the Dark Web in a bulk package for US$200,000 (Goel, 2017). It is important to consider that such a package is not only sold once but multiple times to whomever is prepared to pay for it. Potential buyers include Spam-as-a-Service providers, for instance, who offer other fraudsters to perform mass send outs of whatever questionable content.

Another example is derived from an examination of DDoS attacks by Noroozian et al. (2016). With DDoS attacks being available starting from as little as US$1.00 for a small-scale attack, the booter services, commonly referred to as DDoS-for-hire services, have drawn more attackers to the DDoS ecosystem. These attacks are infrequently employed for attacks on high-value targets such as financial institutions or governmental entities. As per the author's findings, more than 60% of the victims are ordinary end users who are basically being knocked off for fun. Because it is cheap and effective, DDoS-ing has become particularly popular among teenagers who may want to hinder other contenders to engage in an e-gaming community or other online forums.

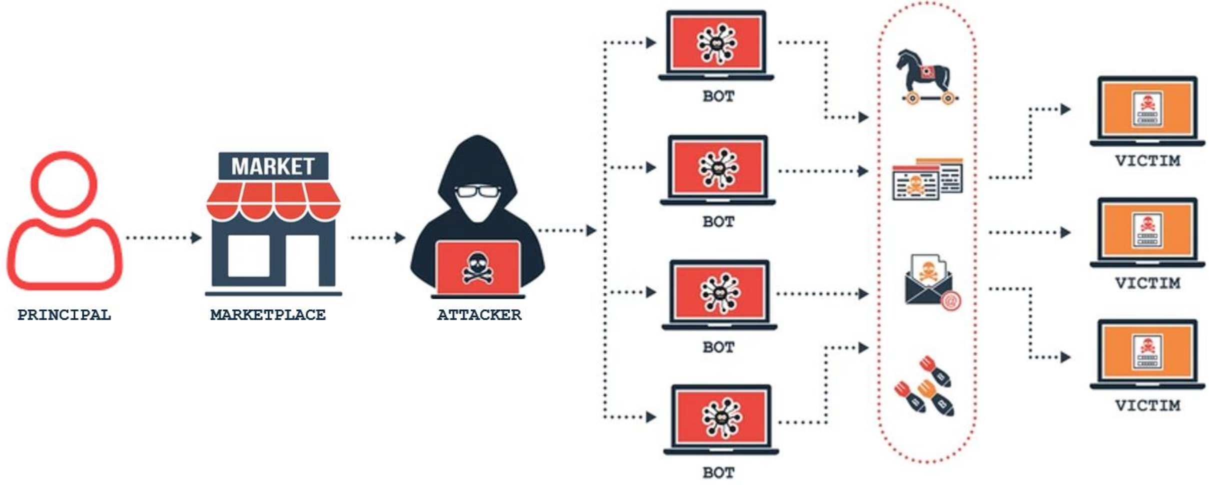
Exacerbating the expansion of the cybercrime ecosystem is not only the availability of illegal services, but also toolkits, and tutorials with a detailed set of instructions for any service or product being sold. Among other things, this includes customizable malware (Malware-as-a-Service) or ransomware affiliate programs that equip the attackers with the ransomware and affiliate software to manage victims. Affiliate programs are the driving-force that fuels the expansion of the cybercrime ecosystem (Europol, 2023b). At the same time, these ransomware schemes forge new supply chains and relationships (Europol 2021a; Robinson et al., 2022; ENISA, 2022). Following the receipt of cryptocurrency payments from the victim, the revenues are automatically distributed among the criminals involved in the attack, including the administrators, the affiliate responsible for carrying out the attack, and the service providers. The affiliate's share of the profit is determined by their rank, which is based on the success rate of their attacks and the amount of criminal profits generated. Initially, the affiliate's share is low, ranging from 20-40% of the ransom, but as they climb the ranks, they can receive up to 80% of the profits (Europol, 2023b). As a force multiplier to "recruit talent", even online training can nowadays be purchased to allow newcomers to improve their hacking skills (Huang

therefore required to determine the impact of competition in underground markets vis-a-vis other factors on the observed price reduction.

& Madnick, 2017). Consequently, conducting a ransomware campaign no longer requires the culprit to have programming skills. Knowing where to purchase the tools and tutorials is all that is needed (Cameron, 2017). As witnessed by law enforcement, there is also increasing collaboration among perpetrators and professionalization of the cybercrime ecosystem (ENISA, 2022a). This not only lowers the entry barriers and allows new entrants with low technical skills to enter the scene and carry out cyber-attacks, but also makes the operations of mature and organized threat actors more efficient (ACSC, 2022; Akyazi et al., 2021; Huang & Madnick, 2017). All this fuels commerce of illegal goods and services and serves as a catalyst to propel further crime (Europol, 2022, pp. 6-17).

One of the prevailing issues with CaaS is, that it makes attribution of cyber-attacks more difficult since it adds another abstraction layer. More precisely, the crime is committed leveraging a third party. The attacker is the one who carried out the crime, but not necessarily the one who sponsored it (otherwise known as the sponsor or principal). These criminal supply chains, make the identification of the perpetrator and principals increasingly more difficult (Bruijne et al., 2017). Since CaaS is a transactional model facilitated in anonymity using camouflage tactics and tools to hide the identities of the involved parties, the CaaS vendor does not know the identity of the sponsor, and vice-versa. To further complicate matters, consider a scenario where a principal in one country hires a cybercriminal in another to carry out a cyber-attack against a company located in a third country. This attack leverages compromised infrastructure via a botnet distributed across dozens of different countries around the globe. Such a botnet can consist of thousands, or even millions, of devices and computers manipulated by the attacker to perform various malicious activities (see Chapter 4.4.3). Even if the attack were later partially traced back to IP addresses in some of these countries, identifying the actual perpetrator becomes a monumental challenge. Tracing the attack back to the cybercriminal who initiated it is already difficult but linking it back to the original principal who ordered the attack adds yet another layer of complexity. In this context, finding the culprit is not merely about locating a needle in a haystack—it is about not even knowing where the haystack is in the first place (see Figure 6). A noticeable achievement took place in 2024, when the FBI apprehended several individuals linked to the 911 S5 Botnet, a malicious network that compromised computers in nearly 200 countries and facilitated various cybercrimes, including financial fraud and identity theft. The botnet controlled millions of residential Windows computers worldwide, connected to over 19 million IP addresses, including 613,841 located within the United States (U.S. Department of Justice, 2024). Unfortunately, such successful investigations are more of an exception than the norm (see Chapter 3.3.4).

Figure 6: Botnet Supply Chain



Source: Author (adapted from Shutterstock)

Akyazi et al. (2021) conducted a longitudinal analysis of the CaaS market by reviewing dataset spanning a period of 11 years of one of the oldest underground forums. Of 28 known CaaS types, they only discovered nine of them in the forum. The authors challenge the widely held view that CaaS was a growing business. They found no supporting evidence for dramatic shifts in these offerings over time, not even after major underground marketplaces were taken offline by law enforcement, suggesting that CaaS *"might not be such a widespread phenomenon as is often assumed"*. These findings must be interpreted with caution and are in stark contrast with other research in this area (Huang & Madnick, 2017; Huang et al., 2018; Nobles et al., 2023) and reporting by law enforcement.[20] However, as already partially acknowledged by the authors themselves, their study has several limitations and drawbacks. They only reviewed one specific underground forum, which does not allow for extrapolation toward the entire CaaS market. Additionally, the authors only analyzed the thread headings and first posts of each thread within the market section of the forum, thus subsequent activity and external links may have been missed. Furthermore, the methodology might be inherently biased and skewed since they focused on one active forum while the most successful underground marketplaces have been seized by law enforcement as evidenced in the following chapter. While the authors have

[20] For example, Europol reported in 2021, that CaaS *"continued to proliferate"* and that *"in the past 12 months, European law enforcement agencies have reported an increase in MaaS offerings on the Dark Web, of which ransomware affiliate programs seem to be the most prominent"*, see Europol (2021a, p. 17). Likewise, the Australian Cyber Security Centre reported in 2022, that the *"evolution of Cybercrime-as-a-Service (CaaS) continued to increase the overall cybercrime threat to Australia"*, see ACSC (2022, p. 38).

highlighted significant observations, additional research in this area is necessary to support and substantiate their conclusions.

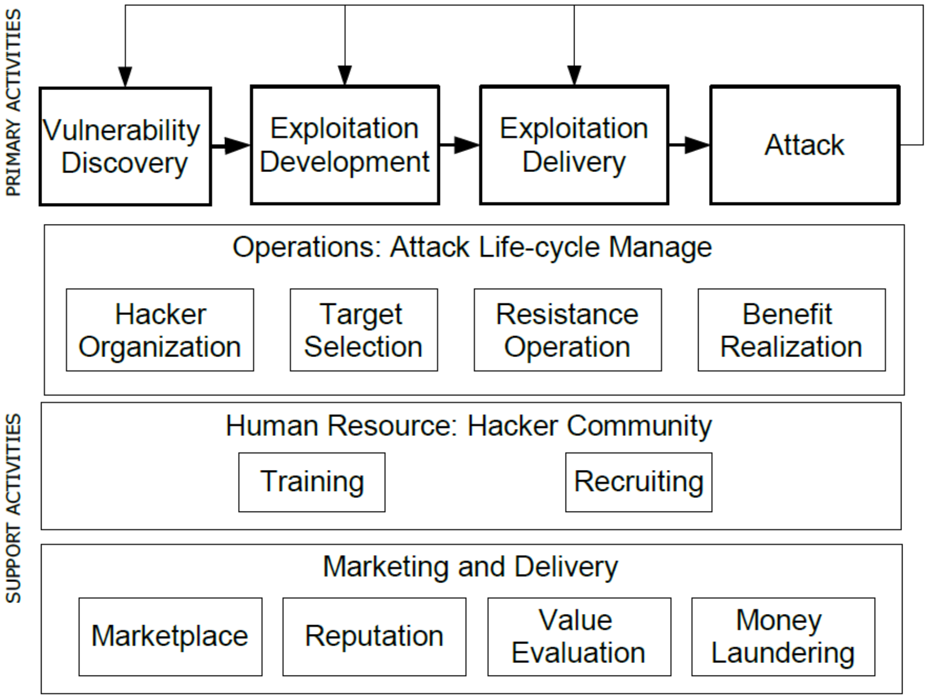
3.3.4. Cybercrime Ecosystem

The proliferation of the Cybercrime-as-a-Service (CaaS) model has made the trade of illegal services and products commonplace. As a natural evolution, some levels of *Industrialization* can now be observed whereby transformation is taking place characterized by increased productivity through professionalization, specialization, and standardization. Instead of putting together products that are individually tailored and manufactured, standardized and off-the-shelf services are now being offered and sold in bulk quantities (mass production).

Cybercrime actors integrate cutting-edge technology into their activities. At the same time, they act as pioneers and seize the opportunity to set up new shell corporations whose illicit business model was made possible in the first place by the internet and the continued growth of e-commerce (Kraemer-Mbula et al., 2013). The underground economy represents indeed a thriving ecosystem which, according to Moore (1993, p. 22), *"like its biological counterpart, gradually moves from a random collection of elements to a more structured community"*, and in which *"companies coevolve capabilities around a new innovation: they work cooperatively and competitively to support new products, satisfy customer needs, and eventually incorporate the next round of innovations"*.

This ecosystem comprises an array of actors who collaborate and trade with one another, various underground forums and marketplaces as well as tools and technologies which build the foundation (see Chapter 3.3.3) or, as Manky (2013) puts it, *"CaaS has become a well-oiled machine, built on a wide network of players that fulfil specific functions"*. This encompasses not only primary activities that are directly linked to cyber-attacks, but also support activities that allow criminals to realize efficiency gains, namely higher revenue, lower operational risk, and reduced expenses. The activities involved in executing cyber-attacks, such as selecting a target, organizing the hackers, realizing benefits, and implementing resistance measures, can substantially enhance the attackers' proficiency in achieving digital, psychological, and financial gains. Besides exploiting technical vulnerabilities, attackers also exploit operational vulnerabilities related to an organization's deficiencies associated with procedures, policies, and personnel. These support functions are often overlooked although they play a critical role in facilitating the underground economy. The cybercrime ecosystem can be imagined as a set of value-added activities (see Figure 7).

Figure 7: Cybercriminal Value Chain Model



Source: Huang and Madnick (2017, p. 4)

This thriving ecosystem as a whole is often collectively referred to as "underground economy" (Anderson et al., 2018; Anderson et al., 2013; Décary-Hétu & Giommoni, 2017; Holt, 2017; Jeffray & Feakin, 2015; Wang et al., 2023), "shadow economy" (Gaspareniene et al., 2016; Gaspareniene et al., 2018) or the "black market" (Delamarter, 2016; Denić & Devetak, 2023; Hatta, 2020; Holt, 2017), characterized by illegal, unreported, or unrecorded internet-based activities, driven by profit, tax evasion or circumvention of legal regulations on commerce and/or business reporting (Florêncio & Herley, 2011; Gaspareniene et al., 2016).[21] For the purpose of this thesis, the terms "underground economy", "shadow economy", and "black market" will be threated synonymously.

Research suggests that the marketplaces in the Dark Web represent an integral part of the cybercrime ecosystem (Wang et al., 2023). As per 2018, there were an estimated 6,000 illegal marketplaces online selling more than 45,000 different products (Lewis, 2018, p. 11). Besides cybercrime products and services, this includes stolen PII data, firearms, ammunition, banned content, illegal substances, and so on (Denić & Devetak, 2023). Case in point, in the context of the Ukraine war, an advertisement for U.S.-donated anti-tank missiles popped up on

[21] For detailed discussion and analysis of the scientific literature about the "digital shadow economy" see Gasparenienea et al. (2015; 2018), and for "underground economy" see Herley & Florencio (2010).

one of the marketplaces in the Dark Web. The item was offered for US$30,000 per piece in exchange for crypto coins, while the item was apparently worth US$200,000. The seller, who claimed to be from Kyiv, supposedly offered transportation of the ordered goods to Poland. Whether this was an authentic offer, a criminal who just wanted to snatch money, or part of foreign propaganda to undermine the Ukrainian government and international support from its allies, remains unclear (Denić & Devetak, 2023, p. 122).

Because the internet never sleeps, all this results in illegal activities around the clock and around globe (see Table 4).

Table 4: Estimated Daily Activity (Extract)

Cybercrime	Daily Activity
Malicious scans	80 billion
New malware	300,000
Phishing [*attacks*]	33,000
Ransomware [*attacks*]	4,000
Records lost to hacking	780,000

Source: Lewis (2018, p. 5)

Given the short existence of certain cybercriminal gangs, core members often promote their skills more widely and may concurrently partake in various underground groups (Europol, 2023b). Investigations against individual criminals have rather low impact in terms of the disruption to the criminal ecosystem. It occupies law enforcement resources with little incentive. Instead, the authorities typically focus on key players who operate a marketplace platform that enable these crimes in the first place (Europol, 2022, p. 17).

For example, between 2011 and 2013, for over two and a half years until its seizure by the FBI, *Silk Road* had debuted as the first illegal marketplace in the Dark Web with significance in terms of size, revenue, and global reach.[22] The advent of *Silk Road* introduced a "new breed" (Décary-Hétu & Giommoni, 2017) of illegal online marketplaces focusing on drugs (Martin, 2014). As highlighted by Aldridge and Décary-Hétu (2014) and Jeffray and Feakin (2015), *Silk Road* was labeled as the "Amazon" for narcotics and considered a "game-changing innovation" at the time irrespective of its condemnable business practice. These underground markets facilitate a form of illicit drug sales that is "qualitatively different" from the offline markets

[22] While *Silk Road* was the authorities primary target, an additional 413 illicit services got shut down in a joint operation, see e.g., Jeffray & Feakin (2015, p. 6) or Décary-Hétu & Giommoni (2017, p. 5).

(Martin, 2014). These platforms do not subsidize traditional drug trafficking but supplement it, for instance by catering to a different audience (Jeffray & Feakin, 2015). *Silk Road* also served as an underwriter for the transaction governing the relationship between seller and buyer. The funds remained in the operator of the website's possession until the illegal goods were delivered (Denić & Devetak, 2023). The marketplace was transactional in nature with most of the items being available for less than three weeks, and many vendors vanishing again within three months after joining (Wang et al., 2023).

With almost 1 million users and some 4,000 vendors registered at the time of its seizure, *Silk Road* is estimated to have facilitated transactions of 9,519,664 Bitcoins worth US$1.2 billion at the time[23] (Denić & Devetak, 2023; Jeffray & Feakin, 2015), translating into more than US$80 million in commissions for the operator, Ross Ulbricht, otherwise known as "Dread Pirate Roberts" (ICE, 2013; Jeffray & Feakin, 2015).[24] Along with the arrest of Ulbricht, the FBI seized around US$33 million in Bitcoin (Décary-Hétu & Giommoni, 2017). Referred to as *"the kingpin of a worldwide digital drug-trafficking enterprise"*, Ulbricht got sentenced to life in prison in 2015 (Weiser, 2015).

In a matter of weeks following the closure of *Silk Road*, a successor marketplace, named *Silk Road 2.0*, emerged. However, during this period, there was strong competition due to other marketplaces that suddenly appeared. Among these contenders, *Sheep* rapidly gained traction but within a couple of weeks, the administrators of *Sheep* abruptly terminated the platform, citing a security vulnerability that had been exploited by a user although many believed this was an "exit scam" by the marketplace administrators who took off with 5,400 BTCs, worth around US$6 million at the time, of their users' money (Aldridge & Décary-Hétu,

[23] The Bitcoin value in 2013 was, with the benefit of hindsight, artificially low with 1 BTC worth US$110. The numbers are even more mind-blowing when taking into account the development of the BTC:USD exchange rate. When quantifying the transaction based on a 2023 exchange of around US$24,000 for 1 BTC, the total value of the Bitcoins exchanged would translate into the astonishing amount of US$228 billion.

[24] Numbers in terms of the success of *Silk Road* vary significantly ranging from 1,000 vendors to 4,000 vendors and an estimated 600% growth from US$14.4 million in 2012 to US$89.7 million in just over a year (Aldridge & Décary-Hétu, 2014) toward US$1.2 billion within two and a half years (Jeffray & Feakin, 2015; Denic & Devetak, 2023). However, the "official" number of transactions facilitated referenced by law enforcement and subsequently referenced during the court trail when criminal charges were put forward against Ross Ulbricht was US$1.2 billion as reported by the United States Immigration and Customs Enforcement (2013).

2014; UNDOC, 2013).[25] While *Silk Road 2.0* remained smaller in scale than the original one, the marketplace was taken offline by law enforcement in less than a year after its launch (UNDOC, 2013).

Such exit scams are not uncommon when it comes to these underground marketplaces. In fact, Wang et al. (2023) argue that a seizure by law enforcement is rather the exception than the norm. Of 21 Dark Web marketplaces analyzed that vanished between 2019 and 2022, only five (24%) were taken offline by law enforcement. Six (29%) were voluntary closures whereby administrators made pre-announcements toward the community before retiring the forum, while the disappearance of 10 marketplaces (48%) was classified as exit scams. The authors acknowledge limitations of their research, especially because of the small sample size relative to the number of available underground marketplaces which inherently might have introduced bias. Several other exit scams followed in subsequent years with administrator vanishing after stealing large amounts of cryptocurrencies from their user community. The issue here is manyfold: Because of anonymity inside the community, the identity of the administrators remains a mystery. Next, as per design, cryptocurrencies are hard to trace, which makes it an enticing endeavor for the administrator to possibly purloin the funds and take off into the sunset. Likewise, because of the criminal nature of the business and the community as such, it makes it practically impossible for the victimized outlaw to report the case and seek help from law enforcement (U.S. Department of Justice, 2014). Though all of this happened online, it is like in the real world with a drug deal gone wrong. In these underground circles, the risk of encountering a “rip-off” may just be part of life (otherwise known as an *externality* in economic terms).

In 2014, the Dutch and German police had successfully shut down *Utopia*, an underground marketplace that facilitated the illicit trade of drugs, stolen credit cards, firearms, and various other illegal commodities. Despite its brief operational period of only nine days, the site had amassed approximately 13,000 listings with a significant number of vendors offering worldwide delivery services (Jeffray & Feakin, 2015; UNDOC, 2013, p. 81). This

[25] Another exit scam took place in 2015, when the *Evolution* marketplace disappeared, with administrators reportedly having stolen US$12 million from their community (UNDDOC, 2013; Aldridge & Décary-Hétu, 2014). In 2020, an even bigger exit scam followed when *Empire Market*, another large-scale marketplace, suddenly disappeared with the administrator having snatched as much as US$30 million from their user community (Wang et al., 2023).

occurrence serves as a testament to the growing prevalence and appeal of such illicit online marketplaces.[26]

Several years later, in 2021, following a cross-border investigation, the authorities shut down *DarkMarket*, which hosted more than 2,400 criminal vendors and an estimated half a million users. According to Europol, more than 320,000 illegal transactions had been facilitated on this marketplace, corresponding to more than €140 million in revenues (Europol, 2021). In another joint operation in 2022, German and U.S. law enforcement agencies took *Hydra Market* offline. According to the U.S. Treasury Department, *Hydra Market* revenues had risen dramatically from US$10 million in 2016 to peak at over US$1.3 billion in 2020 prior to the crackdown (U.S. Department of the Treasury, 2022). It was widely labeled as *"the world's largest and most profitable illegal marketplace"*. Trading on the platform included Ransomware-as-a-Service, hacking services and software, stolen PII data, counterfeit currency, stolen cryptocurrencies, and illegal drugs (ibid.). Until its demise, it served as a mega shopping mall for criminals around the globe. Analyst firm Chainalysis concludes that *Hydra Market* stood for around 93% of all illegal markets on the Dark Web, and that following the demise of *Hydra Market*, total spending on the Dark Web temporarily plummeted from US$3.1 billion in 2021 to only US$1.5 billion in 2022 (FE Digital Currency, 2023). Notwithstanding the above, despite the noticeable success manifested in the seizure of the infrastructure along with US$25 million in cryptocurrencies, arrests are yet to be made. Law enforcement voiced concerns that the gang behind *Hydra Market* will probably continue to operate and might resurface (U.S. Department of the Treasury, 2022; Wang et al., 2023).

These revenue numbers of these marketplaces appear even more astonishing when making present that these underground forums can hardly run any conventional marketing campaigns and largely depend upon word of mouth instead to win new customers.

In 2023, authorities first knocked off *Monopoly Market* during what was codenamed "Operation SpecTor". More than US$53.4 million in cash and cryptocurrencies, along with 850 kg of narcotics, and 117 firearms were seized by police forces across Austria, Brazil, France, Germany, Poland, Switzerland, the Netherlands, the United Kingdom, and the United States (Europol, 2023a). A few months later, "Operation HAECHI IV" was conducted, leading to the capture of around 3,500 individuals who were believed to be participating in a major online

[26] For further discussion about the illicit trade of narcotics on the Dark Web see e.g., Aldridge & Décary-Hétu (2014), Martin (2014), Décary-Hétu & Giommoni, (2017).

fraud operation. This operation also resulted in the seizure of a staggering US$300 million, which was suspected to be linked to the illegal activities of the scam (Interpol, 2023).

Despite these remarkable successes by law enforcement outlined before, they mark only the tip of the iceberg. The Dark Web marketplaces are frequently compared to a mythical creature known as the "Greek hydra" due to their ability to regenerate. Once a head has been cut off, two new will regrow, thereby illustrating the dilemma of a "cat-and-mouse game". Crimes committed in the Dark Web share similarities with those in the physical world, but the primary obstacles stem from the extensive scope, unpredictable characteristics, and the veil of secrecy provided by Dark Web platforms. This makes it difficult to identify, combat, and prevent criminal activity. New underground forums steadily appear to compete with existing ones and replace those shut down (Denić & Devetak, 2023; Wang et al., 2023).[27] There is no such thing as a vacuum. Users too are inclined to simply move on to a substituting marketplace when another marketplace goes offline (Wang et al., 2023). Similarly, Kadlecová (2015) notes that several Russian underground forums had been removed but the most popular ones simply changed their domain names and hosting providers and resurfaced. Also, in the context of child exploitation communities on the Dark Web, Europol acknowledges *"considerable resilience in response to law enforcement actions targeting them. Their reactions include resurrecting old communities, establishing new communities, and making strong efforts to organize and administer them"* (Europol, 2022, p. 21). This does not come as a surprise when taking into consideration the profitability of these criminal activities combined with a low probability of being caught (see next chapter). When considering the anecdotal evidence, it suggests that the marketplaces only grew bigger in size over time in terms of revenue and vendors relative to their predecessors, thereby indicating the increase of illegal trade volumes on the Dark Web.

3.3.5. Cybercrime Rationale

The widespread use of technology and the growing rates of internet connectivity around the globe coupled with the continued development of new technologies that allow for anonymity on the internet have made cybercrime a toxic combination of a low-risk, high-yield venture for a diverse range actor (Peters & Jordan, 2020). A proficient street criminal in the terrestrial world might be able to rob multiple victims a day, but it seems mediocre relative to the scale effects of cybercrime (Topalli & Nikolovska, 2020). In this regard, cybercrime can be a lot more efficient and lucrative.

[27] For general discussion about the lifespan of illegal underground marketplaces see Wang et al. (2023)

In traditional forms of crime, most offenders have limited education and labor market skills, poor employment records, and low legitimate income (Freeman, 1999). This is contrary to cyber-threat actors. New research gives “strong indication” for the idea that cybercriminals’ intellectual capabilities differ from those of ordinary criminals and are in fact higher (Schiks et al., 2022). Further empirical research is required to both confirm the differences in intellectual capacity and investigate additional traits that might set cybercriminals apart from other offenders. Notwithstanding the forgoing, anecdotal evidence seems to further support this hypothesis. For a cybercriminal to be successful, it appears intuitively clear that one needs to be computer-literate and tech-savvy which, in turn, needs analytical skills and intellectual capabilities. Unlike in conventional crime, just being a *street-smart thug* will not be sufficient.

One research group concludes that some cybercriminals can earn more than US$100,000 a year by simply trading ransomware kits, which is nearly twice the annual salary of a software developer in Eastern Europe (Cameron, 2017), where many of the perpetrators reside (Das & Nayak, 2013; Lewis, 2018). The United Nation’s Office on Drugs and Crime even refers to the existence of “cybercrime hubs” in Eastern Europe (UNDOC, 2013, p. 34). This is, according to Kadlecová (2015), not just a coincidence but the result of ongoing emphasis on technical education across Eastern Europe in the post-Soviet area. Excessive supply of talent outweighs demand within some regional ICT markets. As such these experts are poorly paid in exchange for their skills and capabilities, the author argues.[28]

Following economic theory, whether to commit a crime is a choice-making process considering Adam Smith’s principle of *rationale self-interest.*[29] As such, in economic terms, a perpetrator decides to commit a crime if the financial gains outweigh the costs (Becker, 1968; Ehrlich, 1996; Probasco & Davis, 1995):

$$M_{b} + P_{b} > O_{cm} + O_{cp} \;\; P_{a} P_{c}$$

M_{b} = The monetary benefits of committing the crime;

[28] One obvious limitation is that the study did not take workforce mobility into consideration. A counterargument can be made that the proposed excessive local supply of cyber-talent is in stark contrast to the widely quoted global talent shortage within the cyber-workforce. Especially when it comes to well-educated STEM graduates, one would assume “brain drain effects”, that is, the emigration of talent. This, while being outside the scope of this thesis, merits further and more nuanced research into the mobility of the cyber-workforce.

[29] Rational self-interest is part of Smith’s Invisible Hand theory. To that end, Smith argued that humans act rationally when making decisions involving their monetary benefits.

P_{b} = The psychic benefit of committing the crime;

O_{cm} = Monetary opportunity costs of conviction;

O_{cp} = Psychic costs of committing a cybercrime;

P_{a} = The probability of arrest;

P_{c} = The probability of conviction.

The formula covers the costs and benefits associated with committing crime. The probability of arrest and the probability of conviction play a significant role in this equation.[30]

Similarly, Gaspareniene et al. (2018) argue that relative to engaging in underground activity, there is a balance of costs and benefits: in this sense, *“[opportunity] costs are borne if a 'shadow' activity has been detected and a person has been punished, while benefits are obtained from evasion of taxes and/or social insurance contributions”.*

Committing offenses is inherently risky, which means, supported by most empirical data, incentives play a crucial role in the decision-making process of the perpetrator (Freeman, 1999). However, when it comes to cybercrime, the response from law enforcement seems to be a drop in the ocean relative to the sheer number of crimes committed. This causes a fundamental problem, that is, that many cybercriminals operate with near-complete impunity (Anderson et al., 2018; Li & Liu, 2021; Singh & Bakar, 2019). Research in the United States, for example, concluded that the likelihood of arresting a cybercriminal is at a marginal 0.03%, thus making it a lucrative endeavor for criminals to pursue their illegal activities (Eoyang & et al., 2018).

In sum, as established before, with too small an opportunity cost due to limited access to legitimate labor as a substitute for crime, coupled with a low probability of prosecution, the grounds for engaging in crime seem plausible. That said, crime is an area of extreme behavior that puts economic analysis to a rigorous test. It seems that the traditional economic thought of *rational self-interest* could reach its limitations when it comes to committing cyber-related

[30] It is worth acknowledging that while economists have made several valuable contributions to the study of crime (e.g., Becker, 1968; Ehrlich, 1996; Freeman, 1999), most research on this topic is contributed by other fields of study. Criminology is a separate field of research bringing together experts from various disciplines such as sociology, psychology, law, and public policy. These researchers contribute insights into the determinants and consequences of crime, as well as the development and evaluation of crime prevention strategies. Professional journals and specialized expertise in criminology further enhance the understanding of crime and its complexities. Collaboration among different disciplines is crucial for a comprehensive understanding of this important societal issue.

crimes. This has to do with the fact that multiple different threat actors operate in the cybersphere. Thus, as outlined before, they are not a homogenous group with identical motives and can neither be treated nor viewed the same. Particularly, when it comes to state-sponsored threat actors, their decision-making process differs from that of ordinary criminals since most of them are politically motivated and not after profits (see Chapter 4.3.7). One could argue that, when contextualizing the thought of self-interest these state-sponsored actors act *irrationally* since they are typically not interested in financial gain. On the other hand, their strategy might still be highly rational, and a set of calculated actions, in line with their respective governments' agenda. Apart from the fact that APT groups use obfuscation techniques and make every effort not to leave a trace, unlike regular criminals, these state-sponsored actors have little to lose and are hardly in any danger of prosecution or arrest since their illicit actions are covered by their respective government which shields the perpetrators when push comes to shove.

3.3.6. Cybercrime Costs

Cybercrime has seen rampant growth effecting citizens and governments alike (Demirdjian & Mokatsian, 2015; Huang et al., 2018). The nature and complexity of cybercrime and cyber-security incidents infer that organizations can witness costs of different types and magnitudes depending upon the type and scale of the activity as well as the size and sector of the organization in question. These illegal activities include thefts, organized crime, paid protection, prohibited manufacturing and sale of products and/or services, smuggling, dummy transactions, bribery, smuggling, and so on (Schneider et al., 2015). However, computing the costs of cybercrime remains a controversial subject.

One approach involves gathering self-assessments from study participants regarding their expenses. However, if any participant underestimates or overestimates the cost, it will inevitably have an impact on the overall figure. Vendors frequently conduct various investigations based on self-estimated individual cases to ascertain the financial ramifications resulting from a cyber-security incident, with the Ponemon Institute serving as a prominent example. The Ponemon Institute's Cost of a Data Breach Report is a widely cited source (e.g., Ament & Jaeger, 2017; Arief et al., 2015; Armin et al., 2015; Bernik, 2016; Frank, 2020; Holt, 2017; Ting, 2019; etc.). Nonetheless, studies related to cyber-security incidents are highly concentrated, making it challenging to obtain a representative sample of the population's losses. Although the Ponemon Institute publishes their report annually, the approaches used in its creation are subject to alterations, resulting in a challenge when drawing comparisons across different years. The Ponemon Institute itself acknowledges numerous limitations such as not testing a non-response bias, thus leaving the possibility that non-participating organization had entirely different cost, among other aspects. All conclusions were drawn on a non-statistical sample of entities. Additionally, since cost estimates can only be positive, such cost studies tend to exhibit an upward bias (Florêncio & Herley, 2011).

In contrast, some scholars use aggregate estimates instead. These estimates suggest that the costs have risen to anywhere between 0.8% to 1.4% of global GDP (Farahbod et al., 2020; Lewis, 2018; Wang, 2019), translating to US$1 trillion in 2020 (Cremer et al., 2022; Hojda, 2022). The mentioned interval is remarkable. According to the World Bank (n. d.), the GDP in 2022 was approximately US$100 trillion. The error margin outlined here, ranging from 0.08% to 1.4% of global GDP, amounts to a staggering US$6 trillion, highlighting the enormous range and imprecision of these estimates. To put the gap in perspective and make the discussion more tangible, US$6 trillion is more than the annual GDP of both Germany and France combined. Similarly, Sviatun et al. (2021) argue that the costs of cybercrime have more than tripled in less than a decade, growing from US$300 billion in 2013 to nearly US$1 trillion in the year 2020. Although this research is inherently valuable, there are limitations within the approach that must be noted. Their research was based upon a comparative analysis of statistical data characterizing the level of cybercrime in the world and individual countries. Among the sources used was a vendor report issued by McAfee, a leading cyber-security firm. Despite being widely cited as a source among practitioners, in the media, and even among scholars (e.g., Cremer et al., 2022; Eling & Wirfs, 2016; Farahbod et al., 2020; Sviatun et al., 2021; Wang, 2019; Willett, 2023), McAfee's approach has been criticized due to poor data quality and inconsistent data (Armin et al., 2015). Such aggregate estimates are often used by cyber-security vendors to urge investment in cyber-security; however, the estimates often lack explicit evidence. Also, incorrect assumptions can easily derail the consideration in question and lead to questionable outcomes. On the other hand, according to publication by the Joint Research Centre (JRC) of the European Commission, the damages to the global economy resulting from the proliferation of cybercrime were estimated to amount to approximately €5.5 trillion in 2020 (Baldini et al., 2020). The disparities in the determination of the figures are striking, as exemplified by more than a five-fold difference between the present examples. There are several reasons for these significant differences, including inconsistent data and varying approaches in the determination of the figures, as well as a considerably large dark figure (see Chapter 3.3.7).

One of the difficulties is that certain types of cyber-security incidents might have subsequent implications in the aftermath (e.g., lack of trust, reputational damages, staff turnover, forensic activities, customer churn, legal fees, litigation, regulatory scrutiny, additional auditing costs, higher insurance premiums, increased spending to build better cyber-resilience, and so on), which are hard to accurately quantify and attribute. Especially the category of “lost business” is often nothing more than a headline. While assumptions may still be made about the duration of an outage, for example by extrapolating financial results (revenue, profit, etc.) per day of business interruption, such estimates are often flawed. In practice, linearity is frequently not observed. Although a single hour out of 2,000 hours might only represent a mere one-twentieth of 1% of the yearly revenue, a five-day (40-hour) disruption could result in a significantly larger impact, exceeding 2% of the total revenue (Franke, 2020; Vecchio, 2016). Therefore, the financial cost associated with a service interruption should be determined by considering its potential consequences at a particular stage in the business cycle including seasonality (Vecchio, 2016). Furthermore, when it comes to pricing in the subsequent loss of trust, such as which business relationships did subsequently not materialize due to reputational damage, one inevitably treads on thin ice and quickly enters the realm of speculation. The temporal delay further complicates such assessments. In a far-reaching, and consequently expensive case, several years may pass between the initial report (and evaluation of the incident) and subsequent legal disputes across multiple court instances and the imposition of fines.

Other scholars have therefore explored different angles and analyzed the costs per record following data breaches (e.g., Algarni & Malaiya, 2016; Layton & Watters, 2014; Lu, 2019; Seh et al., 2020). While this methodology focuses on individual costs per hazardous event, the inherent criticism of the procedure lies in the fact that only data breaches are analyzed. Although these events are arguably among the costliest cyber-security incidents, they represent only a fraction of all malicious events and cannot be generalized to the entire population. Therefore, this procedure is unsuitable for making general statements or assumptions about total costs of cybercrime.

Another stream of studies have been undertaken to determine the financial damages resulting from cyber-security incidents in publicly traded companies by analyzing the stock prices following the disclosure of such events (Ali et al., 2021; Campbell et al., 2003; Hovav & D'Arcy, 2003; Johnson et al., 2017; Xu et al., 2019). However, it is worth highlighting that, beyond mere sentiment, the share price of a firm is influenced by a myriad of factors. This includes fundamental factors (e.g., industry outlook), technical factors (e.g., chart patterns, momentum, etc.), and behavioral factors of traders and investors which have an impact on demand and supply of a given stock. This makes accurately drawing conclusions on the share price’s performance ambiguous (Dieye et al., 2020). Therefore, while a stock’s price may serve as a useful indicator, it does not accurately reflect the true internal costs incurred by the company, nor does the performance of a single stock provide a reliable basis for projecting outcomes across the broader market.

The measurement of cybercrimes is further complicated due to the frequent violation of jurisdictional boundaries, which hinders the collection of accurate statistical data (Levi, 2017). Another important factor in estimating the costs of cybercrimes is the presence of *externalities*, which are often overlooked. These *externalities* can result in productivity losses and indirect costs for third parties who are affected by cyber-security incidents (see *spillover effects* in Chapter 5.4). Although the damage is present, it is not considered when solely calculating the costs of the victim organization. Additionally, governments establish significant organizations and structures to combat cybercrime and maintain control over the situation. The police maintain specialized cybercrime units and personnel, while prosecutors and courts handle legal proceedings. Regulatory authorities have staff and experts to conduct audits and initiate penalty procedures. All these efforts result in state expenditures (taxpayer money) that are rarely mentioned.

While quantifying the damages caused by cybercrime remains difficult, the fact that cybercrime is a surging threat is undeniable (Arief et al., 2015). However, "*measurement is not straightforward, as cybercrimes frequently cross jurisdictions, and the available statistics are fragmentary*" (Anderson et al., 2018). In conclusion, despite the availability of various methodologies and frameworks to compartmentalize the costs of cybercrime, they each come along with an inherent set of limitations. These constraints present in current research necessitates to develop models that can provide a yardstick of the costs associated with cybercrime (Holt, 2017). Consequently, it does not come as a surprise that very few organizations fully comprehend the material implications resulting out of a cyber-security incident (Levi, 2017; Lis & Mendel, 2019).

3.3.7. Dark Figure

Relative to crime, the so-called *dark figure* is a term that describes the number of committed offenses that are never reported or never discovered, which in turn casts doubt over the efficiency and effectiveness of the subsequent analysis and the conclusions drawn from it. While the prevalence of cybercrime and its severe economic implications are widely acknowledged, the lack of data on offenses remains an issue (Kleinewiese, 2022; Levi, 2017; Mehta, 2019). A considerable portion of losses goes unnoticed, while another portion remains undisclosed (Rhee et al., 2012). The reason for cybercrime often going unreported is that victims either do not notice the attack or regard it as not significant enough to warrant a complaint (Arief et al., 2015; Cliff & Desilets, 2014; Dennis et al., 2003). Others fail to report cases because the victims may consider the crimes embarrassing. In the UK, for example, less than one percent of adult internet users report a data breach to the police, while businesses report just under two percent of cyber-security incidents. Within the European Union, a significant proportion (77%) of individuals across a large sample size (n = 27,607) lack awareness regarding the procedures to report a crime, indicating a lack of knowledge about the available channels for reporting criminal activities. Moreover, a substantial majority (70%) refrained from reporting incidents of cybercrime, highlighting a concerning trend of underreporting such offenses (European Commission, 2020). Part of the reason for such low levels of reporting is likely to be the victims' assumption that there is little that law enforcement could or would do (Jeffray & Feakin, 2015). Similarly, the FBI estimates that around 90% of all cyber-related offenses remain unreported (Mehta, 2019). This makes the current reporting of cyber-related crimes fragmented and insufficient (Anderson et al., 2013), and leads to a big dark field of cybercrime incidents that never make it to surface (Kleinewiese, 2022; Tcherni et al., 2016). Still, the crimes that are disregarded have an economic and social bearing, and it is important to come up with methodologies to understand their impact (Mehta, 2019).

The implications of this dark field of cybercrime are profound. The underreporting and lack of visibility contribute to an underestimation of the true scale of cybercrime, which in turn distorts perceptions and leads to judgmental errors such as regression bias, the presence of an availability heuristic, and unwarranted optimism. This distortion in understanding can cause organizations to underestimate the risks and consequently implement insufficient safeguards. As a result, there is a real danger of underinvesting in cyber defense, leaving organizations more vulnerable to attacks than they might otherwise believe.

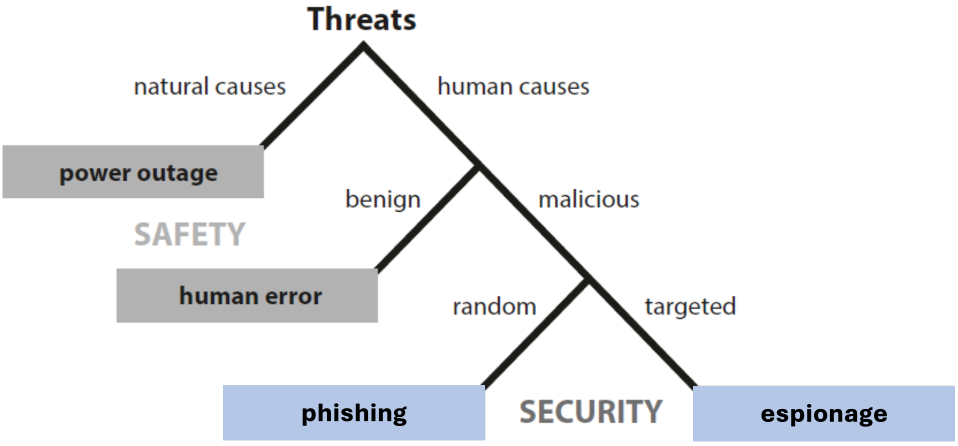
To adequately monitor cybercrime in the future, standardization, and uniform categorization of cyber-related crimes on an international basis are one obvious direction that should be taken. This would help to resolve inconsistencies and, in turn, achieve better quality of data and improve reporting (Bergh & Junger, 2018). Some go one step further and suggest even mandatory reporting of cyber-related incidents (Cremer et al., 2022). Otherwise, fragmented, and inconsistent data has implications for governments and society. Government officials and public institutions rely on crime statistics and related data for policymaking and resource allocation. After all, crime is an *externality* and safeguarding the public and enforcing the law are some of the government's fundamental responsibilities. However, the absence of reliable data impedes the implementation of countermeasures (Armin et al., 2015; Smith, 2006).

CHAPTER 4
THE THREAT LANDSCAPE

4.1 Cyber-Threats

The basic threats in cyberspace include foreign threats, insider/internal threats, threats in the supply chain of goods and services, and threats due to mediocre operational capability of local forces. As pointed out by Herrmann and Pridöhl (2020), to set the stage and contextualize, there is a distinct difference between *safety* and *security*. As such, threats typically related to human life, the environment or equipment can affect (physical) *safety*, whereas the availability, integrity and confidentiality of a given ICT infrastructure relates to *security* (see Figure 8: Safety versus Security). Cyber-threats in that sense, whether random or targeted, are therefore security concerns, and thus addressed though the *cyber-security* domain.

Figure 8: Safety versus Security



Source: Herrmann and Pridöhl (2020), p. 15

According to Li and Liu (2021), cyber-threats are “any event with the ability to strike a blow to missions, tasks, images, national cyber assets, or personnel through an information system, through unauthorized access, destruction, disclosure, alteration of information and/or obstruction of (disruptive) service delivery”. Though the cyber-threat landscape is not static and evolves over time, as established before, existing as well as new cyber-threats can broadly be grouped into three different categories: those targeting the *Integrity* of a given IT system or network, those going after the *Availability*, and lastly those aiming to breach the *Confidentiality* (see Table 5).

Table 5: Cyber-Threat Matrix

Category	Sub-category	Examples
Integrity Cyber-attacks may use hacking techniques to modify, destroy or otherwise compromise the integrity of data.	Propaganda/disinformation Modification or manipulation of data or introduction	Modification or manipulation of data or introduction of contradictory data to influence a political or business outcome or destabilize a foreign regime
	Intimidation	Attacks on websites to coerce their owners (both public or private) into removing or modifying content, or pursuing some other course
	Destruction	Permanent destruction of data to hurt competitors or attack foreign governments. This may, for example, form a part of wider conflict.
Availability Denial of service attacks by botnets, for example, may be used to prevent users from accessing data that would otherwise be available to them.	External information	DDoS attacks on government or private services available to the public, for example, media outlets, government information sites, etc.
	Internal information	Attacks on private or governmental intranets, for example, emergency services networks, energy and transport control infrastructure, e-banking sites, company email, command and control systems, etc.
Confidentiality Cyber-attacks may target various types of confidential information, often for criminal gain.	[*Cyber*-]Espionage	Firms seeking information on their competitors; states involved in spying activities (against both foreign states and individuals)
	Personal data theft	Phishing attacks (or similar) aimed at tricking users into revealing personal data, such as bank account numbers; viruses that record and upload such data from a user’s machine

	Identity theft	Trojan horses, and so forth, used to steal identity information that is then used in the commission of crimes
	Data mining	Open-source techniques employed to discover, for example, personal information from publicly available data
	Fraud	Often delivered via spam e-mail, fraud includes the popular Nigerian “419” or advanced fee fraud, as well as attempts to convince recipients to buy a range of fraudulent goods or services

Source: cf. Buckland et al. (2015, p. 14)

4.2 Ransomware

Although cyberspace is evolving at a fast pace, one constant remainder is the threat that ransomware poses to economy and even physical safety. With the first attack dating back to 1989, ransomware can hardly be deemed a new threat (Duong et al., 2022; Robinson, 2022). Nonetheless, ransomware is still one of the main hazards that organizations must contend with, and it is not anticipated that it will disappear any time soon (Duong et al., 2022; FBI, 2021; Potamos et al., 2023; Verizon, 2023).[31] At present, ransomware is the most prominent type of malware, restricting or preventing access to data and systems. A ransom is then demanded for the release. Such malware either blocks complete access to the system or encrypts certain user data. Ransomware is typically installed using a trojan or a worm deployed via phishing or by visiting a compromised website (Canadian Centre for Cyber Security, n. d.).

The ransomware business has undergone a process of professionalization in recent years, with threat actors refining their tactics and strategies. There has been a shift away from the indiscriminate and haphazard approach of “spray and pray” toward targeting specific enterprises (otherwise known as *big game hunting*) which allows them to extort larger sums of money from their victims (Duong et al., 2022; Richardson & North, 2017). This evolution in

[31] For detailed study about the historic evolution of ransomware and the protective measures that can be taken to mitigate risk, see e.g, Richardson & North (2017), Duong et al. (2022), or Robinson et al. (2022).

the tactics of ransomware actors has significant implications for the cyber-security landscape and underscores the need for robust and proactive measures to counter this threat.

Meanwhile, ransomware attacks are often conducted using *double-extortion*, in which, beyond initially encrypting the victim's data, sensitive data is being exfiltrated, giving the perpetrator additional leverage to demand further ransom payments in order not to leak the stolen data publicly with Maze being one such example of a double-extortion ransomware code (Kerns et al., 2022). This is especially dangerous for organizations since the original ransom attack not only hampers business operations, but the prospect of leaked data could make matters worse and potentially translate into reputational damages, regulatory fines and severe legal fees following a class-action lawsuit. As highlighted by ENISA, in 2021, the identities and proof of compromise for 2,566 victim organizations were publicly announced on ransomware leak sites, representing an 85% increase compared to 2020 (ENISA, 2022a, pp. 9, 73). The ransomware onslaught is indeed a global problem (Richardson & North, 2017). Estimates are that there are some 6,300 underground marketplaces offering ransomware-related services and products (Cameron, 2017). Law enforcement agencies from around the world (including Australia, Europe, and the United States) have uniformly reported a surge in global ransomware campaigns plaguing a variety of different industries (ACSC, 2022; ENISA, 2022a, pp. 9, 75; Europol, 2022, p. 21). As a matter of fact, even the U.S. Marshall Service itself got hit by a ransomware attack in 2023, exemplifying that nobody is immune against cyber-threats, causing the agency's IT system for tracing fugitives—often accessed on behalf of state and local law enforcement agencies—to be unavailable for ten weeks (Barrett, 2023).

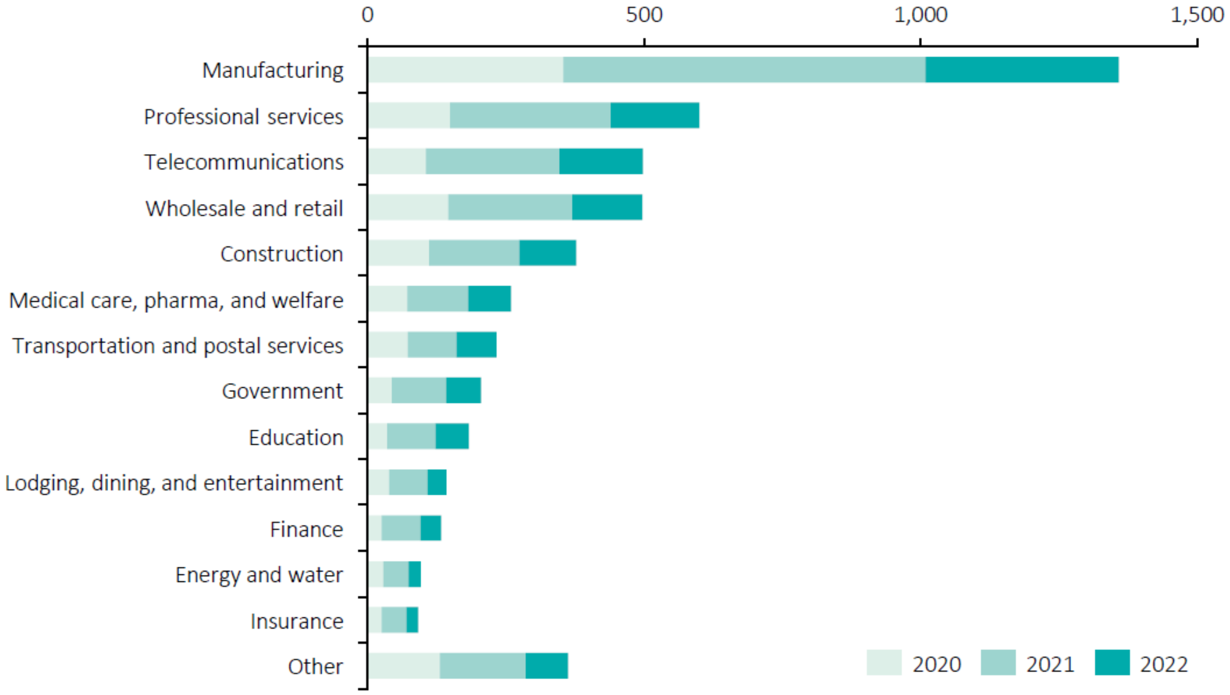
One step further beyond *double-extortion* goes *triple-extortion*, whereby the victim organization receives distributed denial of service (DDoS) attacks, thereby making websites and other critical services unavailable to reinforce the perpetrator's claims (Europol, 2022, pp. 8, 21; Robinson, 2022). When a DDoS attack occurs in connection with ransomware or when a ransom payment is demanded in order not to launch a DDoS attack, the scheme is referred to as RansomDoS or RDoS in short. Consistent with that, Europol notes that *"DDoS for ransom seems to be making a return as criminals use the names of well-known advanced persistent threat (APT) groups to scare their targets into complying with ransom demands"* (Europol, 2022, p. 20). It remains questionable whether these APT groups are really behind these campaigns since they normally conduct more sophisticated attacks. As already pointed out by law enforcement, it seems more likely that criminals simply use *free rider effects* by associating themselves with these APT groups as well as their infamous "brand reputation" and "track record" to intimidate victims and increase the odds of receiving a payment.

What has already been common practice across the software industry can now be observed in the shadow economy, too. Instead of demanding a one-time ransom (basically the equivalent of a perpetual licensee in a legitimate business context), RDoS offenders have begun introducing a "subscription-based model" in which an ongoing ransom fee, e.g., 1 BTC a day, is demanded as protection money in order not to strike an attack (ENISA, 2022a, p. 73). Consistent with reports from law enforcement and as highlighted by Robinson (2022), *quadruple-extortion* schemes have meanwhile emerged, whereby—as an extension of the concept of *triple-extortion*—criminals add strategies of a supply chain attack by expanding their malicious actions toward the victim organization's customers or suppliers to exude even more pressure (Europol, 2022, p. 21; Robinson, 2022).

From an academic perspective, Richardson and North (2017), argue that, in realization that different parts of the word have different willingness to pay, ransomware gangs already practice yield management (otherwise known as variable a pricing strategy, based on geography, understanding, anticipating, and influencing consumer behavior) in their demands. Another example of yield management has been observed by Huang and Madnick (2017), when one ransomware exploit kit (named "Angler") was temporarily unavailable, the demand for a substituting exploit kit ("Neutrino") increased so heavily that the developer just doubled the price from US$3,500 to US$7,000 a month. The same authors computed the costs of running a fictive ransomware business by assembling the different components needed which are all part of the comprehensive cybercrime-as-a-service portfolio. As per their findings, the basic expenses would translate into approximately US$14,000 per month. Assuming a nominal success rate of 10% and deducting the costs including 40% commission for leveraging money laundering services, it would still be absurdly profitable, producing almost 13,000% return on the investment made. While this is a back-of-a-napkin calculation and of indicative nature only, it illustrates how lucrative this questionable business practice can be.

Similarly, Hernandez-Castro et al. (2020) performed an economic analysis of ransomware as a source of income, scrutinizing the illegal gains of the criminals in conjunction with different attack strategies deployed, modeling how criminals could further increase their profits through further price discrimination. In general, ransomware attacks have witnessed a surge on the back of the COVID-19 pandemic and the accelerated adoption of digital technology (Alqahtani & Sheldon, 2022; Duong et al., 2022). However, certain industries have been hit harder than others. According to a study conducted by Deloitte, from 2020 to 2023, double-extortion ransomware has particularly plagued the manufacturing sector by a large margin, followed by professional services and telecommunication services on a par with wholesale and retail (see Figure 9).

Figure 9: Number of Companies globally hit with double extortion Ransomware



Source: Deloitte (2022, p. 8)

Over the past couple of years, ransomware has constantly ranked among the costliest cyber-threats with WannaCry and NotPetya (see Chapters 4.2.1 and 4.2.2 respectively) being two recent variants that caused wide-ranging havoc and huge financial ramifications around the globe. IBM quantifies the average total cost of a ransomware attack at US$4.54 million without taking the actual ransom payment into account (IBM/Ponemon Institute, 2022, p. 6). The duration of such a ransomware attack is a pressing concern due to its considerable impact on businesses, as it lasts an average of 23 days (Coveware, 2021). This prolonged period of operational downtime poses substantial challenges for affected organizations, resulting in significant financial losses and operational setbacks. To make the business impact more tangible, when assuming a linear operation of 365 days per year, the 23 days of downtime within that period would result in a loss of 6.3% of the annual revenue and profits. This calculation does not include the costs of restoration, legal fees, regulatory fines, and long-term damage to the company’s reputation. If the company operates only 280 working days per year, the same amount of downtime would already translate into a loss of 8.5%. Thus, the costs can quickly escalate depending on the scale and size of the organization. Moreover, in addition to the immediate financial ramifications, the loss of valuable data can be particularly painful. On average, a mere 65% of the data will be successfully restored, with 29% of companies recovering less than half their data in the aftermath of such an incident. This, in turn, makes it imperative for organizations to have a robust backup plan in place (Adam, 2021). This includes regular backups, offsite storage, and testing of the backup system to ensure its effectiveness.

As concluded in a report issued by cyber-security firm CrowdStrike, the average ransom payment increased by 63% in 2021 to US$1.79 million, compared to US$1.10 million in 2020. The average ransom demand from criminals was US$6 million (Crowdstrike, n. d.).[32] From a perpetrators' perspective, ransomware seems to be particularly lucrative and successful with 60% of victimized organizations having paid ransom demands (ENISA, 2022b).[33] In 2020, according to the U.S. Treasury, ransomware payments reached over US$400 million, more than four times their level in 2019 (U.S. Department of the Treasury, 2020b). As reported by FinCEN, the amount surged to nearly US$1.2 billion the following year in 2021, almost three-times the amount of US$416 million in 2020 (U.S. Department of the Treasury, 2021).[34] When putting these numbers officially reported by the authorities into perspective, this suggests that ransomware payments would have effectively witnessed a staggering 12-fold growth over as little as two years from around US$100 million in 2019 to US$1.2 billion in 2021. At the same time, the U.S. authorities estimate that these payments represent just a fraction of the economic damages caused (U.S. Department of the Treasury, 2020b).

[32] Additional uncertainty arises from a multitude of data sources. Different cyber-security vendors publish threat reports with differences in demographics of the cohorts including the composition of industries and countries, methodologies applied, sample sizes, and so on. While CrowdStrike has been chosen, other vendors tend to provide different data points with some estimating the damages per organization exponentially smaller or larger. For instance, Europol (2021a) quantifies the average paid ransom in 2020 with US$312,493 per victim while stating a 170% increase over 2019, reciting an underlying vendor report issued by Palo Alto Networks.

[33] The findings of this study must be seen considering some limitations. In the absence of a single source providing insights on the costs of the ramifications along with the average ransom payments made, the two vendor studies mentioned serve as proxies. The studies—irrespective of possible limitations and biases within each of these studies—are based on different cohorts. Therefore, no further attempts have been made by the author of this thesis to add values from both studies to derive at total costs.

[34] The Financial Crimes Enforcement Network (FinCEN) is a bureau of the United States Department of the Treasury that collects and analyzes information about financial transactions to combat domestic and international money laundering, terrorist financing, and other financial crimes. Established in 2002, pursuant to Section 362 of the U.S. PATRIOT Act, financial instructions are obliged to report suspicious activities to FinCEN that warrant immediate and enhanced scrutiny.

However, fulfilling the demands and making a payment remains a delicate endeavor. Not only does this support the criminal business model and encourage perpetrators to conduct further crime, even worse, there is no guarantee that the victims will regain access to their corrupted files. Multiple cases have been reported whereby no decryption key was provided following the payment (Nobles et al., 2023; Richardson & North, 2017). A separate empirical study comprising 5,400 IT decision makers in mid-sized organizations across 30 countries worldwide concluded that a mere 8% of victim organizations managed to get back all their data after paying a ransom, with 29% getting back no more than half of their data (Sophos, 2021). This does not come as a major surprise since the perpetrators do not embody the idealized role model of honorable merchants. These are ruthless criminals after all, and these individuals are not exactly trustworthy.

The prospect of a decline in the ransomware menace appears to be distant. Experts anticipate that the situation will not improve anytime soon. Despite 77% of professionals acknowledging an enhanced capacity to safeguard against ransomware in the last year, almost half (45%) of cyber-security and IT executives anticipate a continued surge in ransomware attacks (PwC, 2023, pp. 2, 85).

4.2.1 WannaCry

In 2017, the WannaCry worm hit the planet and infected between 200,000 and 300,000 computers across 150 countries (Chanlett-Avery et al., 2017; Harknett & Smeets, 2022; Willett, 2023) within a matter of days (Lis & Mendel, 2019).[35] The malicious code restricted users' access to a computer until a ransom was paid to unlock it. WannaCry was initially delivered through phishing attacks and spread like wildfire as it exploited security vulnerabilities to move remotely between unpatched computers. The United States government attributed the global attack campaign to a North Korean state-sponsored threat actor and put criminal charges forward against several suspects who were linked with the widely known *Lazarus Group* (see also Chapter 4.3.7). This APT group was also made responsible for other high-profile incidents such as the cyber-attack on Sony Pictures Entertainment in 2014 and the exploitation of the SWIFT messaging system between 2015 and 2018 (U.S. Department of Justice, 2018b). The

[35] Some researcher state contradicting and smaller numbers, such as Brar and Kumar (2018) for example, suggesting that 90,000 computers across 99 countries got infected by WannaCry. However, the ballpark of research (e.g., Chanlett-Avery et al., 2017; Harknett & Smeets, 2022; Lis & Mendel, 2019; Willett, 2023; among others) references the spectrum cited.

WannaCry attack also impeded critical infrastructure (see Chapter 5.5), resulting in estimated damages exceeding US$5 billion (Harknett & Smeets, 2022; Lis & Mendel, 2019).

4.2.2 NotPetya

Initially targeting the Ukrainian critical infrastructure, the Russian intelligence service released NotPetya in 2017 and literally opened a can of worms, ushering a new kind of state-backed cyber warfare (Harknett & Smeets, 2022). After ingesting malicious code through a backdoor into a software widely used across the Ukraine to file tax reports, a domino effect was triggered, causing the spread of malware across multiple organizations including Ukrainian subsidiaries of multinational corporations. The malware wiped data beyond repair. While a FedEx subsidiary was unable to take and process orders, shipping company Maersk was brought to a standstill causing wide-ranging *spillover effects* across multiple sectors. Other companies that encountered business disruptions included Beiersdorf, Mondelez, Nuance, and Reckitt Benckiser. NotPetya's damage extent has been estimated differently, but it is widely considered the most destructive cyber-campaign in history. The Federal Reserve Bank of New York determined that the overall economic losses amounted to a minimum of US$7.3 billion (Crosignani et al., 2023). The White House, on the other hand, has projected more extensive damage than initially believed, estimating the total harm to surpass US$10 billion (Wolff, 2022). Indeed, the magnitude of the NotPetya attack was unparalleled. The malware campaign had a far-reaching effect on numerous organizations across more than 60 countries (Wolff, 2022). While Stuxnet (see Chapter 4.3.7) was previously utilized as a cyberweapon jointly attributed to the United States and Israel to sabotage an Iranian uranium enrichment facility, NotPetya went much further and was geared toward widespread collateral damage across critical infrastructures and civilian facilities against a sovereign state during peacetime (Krasznay, 2020). In contrast to Stuxnet's surgical precision, NotPetya can be likened to a sledgehammer exuding nothing else but blunt force.

Welburn and Strong (2022) proposed a comprehensive quantitative model to estimate the cascading effects of cyber-security incidents and concluded that the total economic cost of NotPetya may have been as little as US$3 billion or as much as US$57 billion. As remarked by Forscey et al. (2022), *"the dramatic range underscores the uncertainties involved in attempting to anticipate the effects and losses of highly consequential cyber events"*.

In May 2023, a New Jersey court found the insurer of pharmaceutical giant Merck & Co. liable to compensate the corporation for US$1.4 billion in losses encountered during the NotPetya attack, thereby rejecting the insurers' argument that the attack was *"akin to an act of* *war normally excluded from coverage"* (Vanderford, 2023). Considering the staggering numbers of this isolated case, paired with the fact that many companies have been impacted, anecdotal evidence proposes that some of the more "conservative" estimates about the total economic damage resulting from NotPetya must be revised upwards.

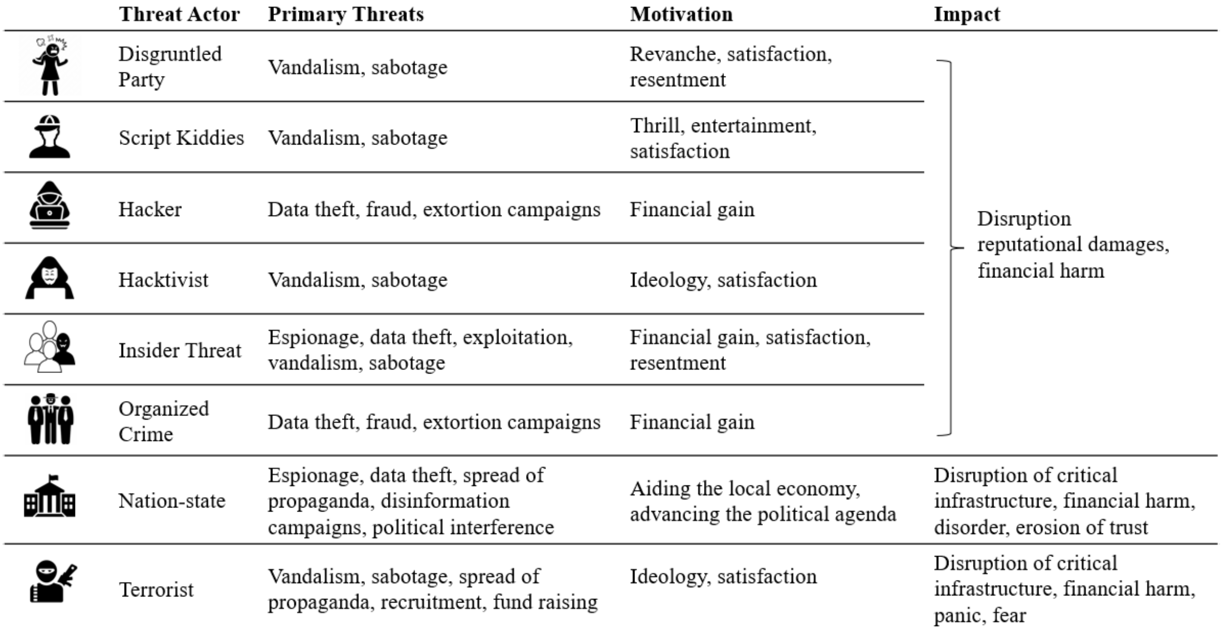
4.3 Threat Actors

Cyber-security is characterized by asymmetries. Threat actors possess a vast array of tactics at their disposal, while defenders are required to meticulously scrutinize every aspect and always remain vigilant. Consequently, the occurrence of successful attacks cannot be solely attributed to victim's negligence (Herrmann & Pridöhl, 2020, p. 11). Besides legitimate users, a confluence of threat actors operates in cyberspace as well. While motives vary, cybercrime is still predominately financially motivated, thus making it an "economic crime". Based upon 2,328 security breaches scrutinized, an overwhelming 94.6% were financially motivated with roughly three-quarters of all incidents attributed to organized crime (Verizon, 2023). Cybercriminals make every effort and are continuously devising new methods to enhance their profit (WEF, 2020).

In essence, the cybersphere extends to the physical world and represents a new realm to conduct criminal activity. When it comes to bad actors, there are distinctively behavioral differences and rich diversity (Buckland et al., 2015). Nonetheless, at the end of the day, their illicit activities, though conducted online, can still largely be grouped into existing forms of economic crime such as fraud, theft, money laundering, and intellectual property crimes (Peters & Jordan, 2020). However, one of the challenges is that different countries use inconsistent methods to identify and categorize threat actors (Bruijne et al., 2017). This lack of standardization complicates international efforts to combat cybercrime, as varying definitions, classification systems, and legal frameworks can lead to misalignment in how threat actors are tracked, prosecuted, and understood. The result is a fragmented approach that can hinder the effectiveness of both national and international cyber-security measures, further contributing to the dark figure discussed in Chapter 3.3.7.

In the absence of a common threat actor typology, the subsequent one will be used for the context of this dissertation (see Figure 10).

Figure 10: Threat Actor Typology



Threat Actor	Primary Threats	Motivation	Impact
Disgruntled Party	Vandalism, sabotage	Revanche, satisfaction, resentment	Disruption reputational damages, financial harm
Script Kiddies	Vandalism, sabotage	Thrill, entertainment, satisfaction	
Hacker	Data theft, fraud, extortion campaigns	Financial gain	
Hacktivist	Vandalism, sabotage	Ideology, satisfaction	
Insider Threat	Espionage, data theft, exploitation, vandalism, sabotage	Financial gain, satisfaction, resentment	
Organized Crime	Data theft, fraud, extortion campaigns	Financial gain	
Nation-state	Espionage, data theft, spread of propaganda, disinformation campaigns, political interference	Aiding the local economy, advancing the political agenda	Disruption of critical infrastructure, financial harm, disorder, erosion of trust
Terrorist	Vandalism, sabotage, spread of propaganda, recruitment, fund raising	Ideology, satisfaction	Disruption of critical infrastructure, financial harm, panic, fear

Source: Author

Further elucidation on these threat actors, their *modus operandi*, and the magnitude of their malevolent undertakings will be expounded upon in the following sub-sections.[36]

4.3.1 Disgruntled Parties

Whether former employees, suppliers, customers, business partners or competitors, various stakeholders can literally turn into a loose cannon, if they are disgruntled and have cravings for revenge. Emotions and irrational behavior play a major role in this regard, especially if somebody feels treated poorly, unfairly or if a business relationship does not end under good terms. Though this was perhaps less of an issue in the past, the emergence of cybercrime-as-a-service turned this from a theoretical problem into a very real one. When a disgruntled stakeholder thinks it is time for retaliation, options are manyfold. As evidenced in multiple cases, it does neither require the perpetrator a great level of technical expertise let alone hacking skills nor big budgets. With little to no effort and lackluster skills, as outlined before, a whole portfolio of different illegal service can simply be procured online and paid on an on-demand basis (see Chapter 3.3.3).

[36] For further study about the cyber-threat actor typology, see e.g., de Bruijne et al. (2017), Brar and Kumar (2018), or Nobles et al. (2023).

In 2017, the FBI charged a Minnesota man for launching hundreds of DDoS attacks on companies all over the world, including his former employers and business partners. The suspect in this case did not bother to access the Dark Web since some DDoS booter services were even available on the clear internet. Several hundred dollars paid to cybercriminals via Paypal and Coinbase where sufficient to cause his former employer losses of over US$15,000 (Cimpanu, 2017). According to a survey of cyber-security firm OneLogin comprising 500 IT decision makers, 20% of organizations polled reported they had witnessed cyber-breaches by former employees (DeNisco Rayome, 2017). The same piece of research also revealed that an astonishing 48% of respondents were aware of their ex-staff's sustained ability to access corporate networks albeit their departure, which poses a major security risk (Golden, 2017).

In some IT-savvy communities and verticals, cyber-attacks, especially DDoS attacks among rivals (sometimes referred to as *Industrial Sabotage*), are nothing uncommon, take crypto-exchanges, online gaming, or e-commerce for example (Ashford, 2017; Copeland, 2020; DataDome, 2020). However, it is worth highlighting that attribution in these cases often remains a challenge. Although there might be some level of indication and it seems plausible, tracing these attacks back to the perpetrator is next to impossible.

4.3.2 Script Kiddies

Generation Alpha is the demographic cohort succeeding *Generation Z,* effectively those born after year 2010. This generation has been growing up amid digital technology. They embrace a digital-first mindset, intuitively control and master devices and software and use them every day. This cohort is also referred to as "screenagers", thereby referencing their technical proficiency and the time they spend in front of their electronic devices. It is the most tech-savvy generation so far, but soon to be surpassed by Generation Beta from year 2025 onward (McCrindle, 2020). Part of this reality too, is that cybercrime unfortunately finds entry into the child's room. Children can fall victim on one hand side (exploitation, cyberbullying, etc.), but they can commit offences on the other hand, too. The term *Script Kiddies (Skids)* has been coined to describe "rookie hackers". It is not uncommon that these kids begin their trajectory with unsophisticated skills but over time quickly progress and often become just as dangerous as their older counterparts. However, they often underestimate the consequences of their wrongdoing. In their research, Santanna et al. (2015) concluded, that *"DDoS-ing became such a widespread phenomenon"* that even school-aged teenagers took their own school offline by procuring DDoS attacks through an illegal booter service. Such cases have been observed repeatedly. For instance, in 2020, while homeschooling was embraced in midst of the COVID-

19 pandemic, a 16-year-old boy from Florida got accused of shutting down his entire school district's remote learning classes on at least eight occasions. Instead of pretending to be sick or not showing up to class, the teenager decided to skip school by DDoS-ing the Miami-Dade's remote-learning platform (Gramenz, 2020). The school district happens to be the fourth largest in the USA. The outage cut off 20,000 teachers and roughly 275,000 students over three days (Wadhwani, 2020). What may begin as a mere prank sometimes culminates in serious offenses. In 2023, an 18-year-old teenager pleaded guilty after hacking some 60,000 user accounts and stealing around US$600,000 from a sports betting website with the defendant bragging prior to his arrest that "fraud is fun" (Mangan, 2023). In a separate case, two other teenagers, aged 17 and 18, were convicted of being part of the cybercriminal group *Lapsus$*. This gang hacked into the systems of well-known Tech firms like Uber, Nvidia, and Rockstar Games. They also infiltrated the servers of British telecommunication giants BT and EE, demanding a ransom of US$4 million (Tidy, 2023b). While the gang's motives varied between fame, money, and amusement, the investigation revealed *"how easy it was for its members (juveniles, in some instances) to infiltrate well-defended organizations"* (CISA, 2023).

In 2022, the United Kingdom's National Cyber Crime Unit (NCCU) reported as much as a 107% surge of young people becoming involved in DDoS attacks. Even more concerning, the average age of referrals to the NCCU was 15, while other offenders were only 9-year-old children (EMCRC, 2022). The troubling results of this study align with another research that found that a considerable 67% of European teenagers (n = 7,974) engage in various forms of online risk-taking including cybercrime (Davidson et al., 2022). Roughly half (n = 3,808) acknowledge involvement in conduct that has the potential to be categorized as a criminal offense. Furthermore, the research stated that a sizeable proportion of young people intentionally conduct their activities in the shadows, with 12% using Dark Web forums, while 11% of these individuals utilize Dark Web underground markets to purchase illicit items (ibid.). The fact that nearly half of the survey participants confessed to engaging in unlawful activities is a significant concern and must not be taken lightly. This issue warrants further investigation into the motives and actions of these individuals, as well as the effectiveness of education and awareness initiatives aimed at preventing such behavior. Since this cohort will soon enter the workforce, there is a considerable peril that their attitudes and online behaviors could elevate organizations to much greater levels of cyber-risks.

4.3.3 Hackers

The term “hacker” is characterized by a lack of clarity, as multiple definitions exist concurrently. Hackers are usually grouped into three distinctive categories, namely *Black Hats, Gray Hats,* and *White Hats*. *Black Hats* embody hackers in the stereotypical sense. They act with criminal energy and have bad intentions. Maliciously breaking into computer networks, stealing data, compromising ICT systems, and seeking personal gain are their bread and butter. These individuals also occasionally release malware that destroys files, takes computers hostage, or steals passwords, credit cards, and other personal information. They act alone or in a collective. For the most part, *Black Hats* are financially motivated. Illicit underground forums and marketplaces for cyber tools and services have made even hackers-for-hire available as a prosperous business model (see Chapter 3.3.3) (Canadian Centre for Cyber Security, n. d.). *Gray Hats,* on the other hand, are actors who violate ethical standards or policies, but without the malicious intent attributed to *Black Hats*. *Grey Hats* may act as hacktivists for ideological purposes, for example. Conversely, *White Hats* (otherwise known as ethical hackers) are hired to legally break into IT systems to assess an organization’s overall security posture and ability to defend. They have the same skills as cybercriminals but adhere to an ethical code of conduct. *White Hats* use their expertise in a good and constructive manner to help organizations rather than harming them. For the purpose of this thesis, when it comes to hackers, emphasis will be put on *Black Hats*.

4.3.4 Hacktivists

Hacktivists operate at the crossroads of hacking and activism. As such, hacktivists engage in disruptive or harmful activities to support a political, ideological, social, or religious cause. *WikiLeaks* and *Anonymous* are notable examples. While many hacktivists try to justify their actions as civil disobedience or anarchism and claim to have noble and altruistic intentions such as promoting equality, justice, or human rights, it does not alter the fact that hacktivism is still a form of cybercrime. Prior to Russia’s invasion of Ukraine, hacktivism had been on a decline with operations remaining low in numbers, capabilities, and impact (Canadian Centre for Cyber Security, n. d.; SecAlliance, 2022). Since then, hacktivism has witnessed a resurgence. *Killnet* is one such collective with pro-Russian affiliations, which actively engages hacktivists in carrying out DDoS attacks motivated by their ideological beliefs. Their main strategy involves promoting the sharing of valuable intelligence concerning potential targets in different countries through dedicated Telegram channels in order to strike attacks (Europol, 2023b). The war in Ukraine has heralded a new era, prompting the involvement of different hacktivist groups that have allied themselves with either side of the conflict and demonstrated sophistication in cyber-operations (ibid.). Both parties have carried out cyber-attacks and, among other things, publicly leaked confidential information related to government agencies, military operations, political bodies, and private companies (Denić & Devetak, 2023). Likewise, the conflict between Israel and its Arab neighbors has attracted the attention of politically motivated hackers, with *Anonymous* claiming responsibility for taking over 100 Israelian websites offline with DDoS attacks, causing temporary disruptions (Bing & Satter, 2023). The prospect of leveraging hacktivists in future conflicts appears quite probable, and if it proves to be effective, it could serve as a new "blueprint" to amplify the impact of such engagements (see *Hybrid Warfare* in Chapter 3.3.2). This, in turn, would have bearing on international norms and laws and might endanger critical infrastructure to greater risks (SecAlliance, 2022; Sentinel Labs, 2022).

4.3.5 Insider Threats

Insider threats have a long political history beyond the cyber-context. Spies divulging information have been a regular theme and subject to counter-intelligence efforts at least since antiquity. Today's insider threats relate to individuals associated with an organization who abuse their privileges to adversely affect the organization's critical information or systems (Collins, 2016), thereby representing a modern form of *"white-collar crime"* (Sutherland, 1940).[37] Financial losses can quickly arise due to insider threats, who hold positions of trust within the company but exploit this trust. These individuals undermine the company by intentionally or unintentionally engaging in actions or errors that have detrimental effects on the firm's well-being. Insider threats are often disgruntled employees. A joint study by Carnegie Mellon University and the U.S. Secret Service found that 1 in 5 cybercrimes were suspected or known to be caused by insiders with factors such as termination of employment and the move to a competitor driving malicious intent (Collins, 2016). Beyond employees, third-party vendors, contractors, and partners can turn into malicious insiders, too (Williams et al., 2019). Whether

[37] Edwin Hardin Sutherland (1883-1950), an American sociologist, considered to be one of the most influential criminologists of the 20th century, coined the term "white-collar crimes", when referring to *"a crime committed by a person of respectability and high social status in the course of their occupation."* This contrasted with "blue-collar crimes," carried out by people of lower social status. Sutherland argued that white-collar crime erodes trust and thus creates distrust, which lowers social morale and produces social disorganization.

premeditated or through negligence, insiders can be particularly dangerous due to their access to internal IT systems that are otherwise protected against the outside world. They may too be associated with another listed type of threat actors or act on their behalf (Canadian Centre for Cyber Security, n. d.). Insider victimization with altruistic intent is typically referred to as "whistle-blowers", arguably with former NSA contractor Edward Snowden being the most well-known example.

4.3.6 Organized Crime

According to the United Nations, organized crime remains a dominant force within the threat landscape, thereby "*substantially diminishing the role of isolated hackers as main actors*" (UNDOC, 2013). Estimates are that somewhere between 80-90% of all cybercrimes involve organized crime in one form or another, thus turning these actors into a major driving force of the underground economy (ibid.). Likewise, a recent study concludes that out of 157,525 cyber-security breaches recorded, 70% were committed by external threat actors with half (50%) being attributed to organized crime groups (Islam et al., 2022). Unlike individual hackers, organized crime groups typically come with planning and support functions and may present themselves to the outside world as a legitimate company (Huang & Madnick, 2017; Huang et al., 2018). However, they operate with bad intent. As such, they conduct cyber-operations at scale, and pocket large amounts of money by utilizing their technical capabilities and targeting victims in bulk quantities. Money is their primary motivation. Nonetheless, organized criminals are not a homogenous group. In fact, much like legitimate businesses, some syndicates have "digitized" their income model more so than others, that is, they are producing a greater share of their revenue streams in cyberspace. These criminals create new markets and subsegments with some operating in a hybrid model comprising both online and offline activities (Kshetri, 2010; Leukfeldt & Holt, 2022). As such, their respective operating model ranges all the way from being *partly*, *primarily*, or *entirely* cyber-driven (UNDOC, n. d.-b). The Russian mafia is one such example of an organized crime syndicate that has meanwhile gained cyber capabilities (Giannangeli, 2008). In the context of illegal drug trading, Ouellet et al. (2022) provide indicative evidence that experience gained in offline settings translates into greater criminal success online. Though based on a small sample size (n = 51), drug dealers who began their career in the physical world tended to outperform those who started off online. As per their findings, those drug dealers who transitioned into cyberspace yielded higher earnings relative to the "digital-first" cohort. This implies that offenders learned from prior crimes and honed their skills to increase future profits.

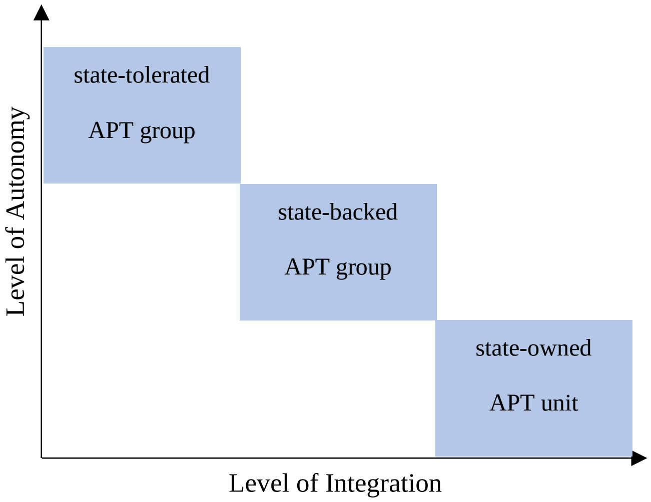
Organized crime groups are often highly specialized with skills in certain disciplines such as conducting scams or running ransomware campaigns, for example (Leukfeldt & Holt, 2022). Especially ransomware groups continue to pose a significant danger as they have successfully developed a well-thought-out strategy to specifically target multinational companies, government organizations, and critical infrastructure (Europol, 2023b). *Fin7* or *REvil* are among the prominent organized crime groups, known for causing extensive damage and racking in large amounts of money. In January 2022, the Russian Federal Security Service (FSB) arrested eight members of the *REvil* ransomware group. The arrested suspects are considered low-level players in the larger *REvil* organization. The possibility of a punitive sentence resulting from the trial is deemed unlikely due to geopolitical tensions (ENISA, 2022a, pp. 46-47). Nevertheless, it is noteworthy that the cybercriminals' actions are influenced by the aggression displayed towards Ukraine as well as the political environment in Russia (Europol, 2023b). The mass mobilization in Russia and imposition of Western sanctions, which includes tech company boycotts, have resulted in a major shift in the criminal landscape of the region. This has offered an opportunity for law enforcement agencies to apprehend high-ranking threat actors who were previously out of their reach. One such instance was the arrest of a prolific Ukrainian cybercriminal who had fled the country in March 2022 and was subsequently captured by the Dutch authorities (ibid).

Global criminal networks have played an increasing role in transforming states, as witnessed in Russia, or some countries across Africa and Latin America, for example, where criminal syndicates have successfully implemented a blueprint for politics, business, and crime to intertwine (Sullivan, 2023). The "new Russia", emerged after the collapse of the Soviet Union, has turned into a new "criminal counter power", that is a new criminal-political ecosystem of *hybrid influence* fueled by corruption (Castells, 2010). In such setups, the demarcation lines between organized crime and state-sponsored activity are blurry. This issue will be further discussed in the following chapter.

4.3.7 State-Sponsored Actors

State-sponsored actors, often referred to as Advanced Persistent Threat (APT), are among the most dangerous and devastating perpetrators, and every so often tasked with advancing geopolitical objectives. Rogue nation states or state-sponsored groups have the resources and expertise to conduct some of the most sophisticated and complex cyber-operations (Canadian Centre for Cyber Security, n. d.; Herrmann & Pridöhl, 2020, p. 17). In many cases, these groups are highly professionalized, well organized and structured in the same way as if they were a legitimate enterprise (Crowdstrike, n. d.). Russia, North Korea, China, and Iran are leading the "wolf pack", followed by Nigeria and Vietnam (Kshetri, 2014; Lewis, 2018; Nobles et al., 2023). Interestingly, there seems to be a tendency of these actors to operate in countries where internet censorship and surveillance are prevalent. This observation implies that the capabilities gained might be used as a "multipurpose weapon" aimed at ensuring obedience domestically toward autocratic regimes, while conducting offensive cyber-operations to advance the geopolitical agenda and aid the local economy. This is an area meriting further scrutiny. It is not uncommon that such APT groups have ties to the military and intelligence services, and either act as a unit within these communities or on their behalf or are funded by them (otherwise known as state-sponsored), or their existence is at the very least tolerated by these authorities (see Figure 11).

Figure 11: Autonomy vs. Integration of APT Groups



Source: Author

The level of intertwining with their government and the operating model of the APT group depends on their respective home country, and even then, the demarcation line can still be fluent. There can also be cases of a more autonomous APT groups being called in upon request to aid their respective government, in exchange for their impunity (Galeotti, 2017). Geopolitical tensions have illuminated the intricate relationships between cybercriminal activities and state-sponsored entities, creating avenues for cybercriminals to achieve financial profit. The linkage between cybercrime organizations and state actors is likely to persist, characterized by a pronounced emphasis on maintaining plausible deniability (ENISA, 2022a).

Taking this into account, it may be prudent for simplification purposes to discern between three different operating models (see Table 6).

Table 6: Typology of APT Actors

Level	APT Actor	Nature of the Actor	Engagement	Integration
1	state-tolerated	Organized crime gang	Occasionally	Low
2	state-backed	Para-military group	Frequently	Medium
3	state-owned	Military/Intelligence unit	Permanently	High

Source: Author

Similarly, Healey (2012) suggests a spectrum of state responsibility that comes along with ten different categories each marked by a different level of responsibility, based on whether a foreign nation state ignores, supports, or carries out a cyber-attack (Table 7).

Table 7: The Spectrum of State Responsibility

Spectrum	Description
State-prohibited	The national government will help stop the third-party operation.
State-prohibited-but inadequate	The national government is cooperative but unable to stop the third-party operation.
State-ignored	The national government knows about the third-party intrusions but is unwilling to take any official action
State-encouraged	Third-parties control and conduct the operation, but the national government encourages them as a matter of policy.
State-shaped	Third-parties control and conduct the operation, but the state provides some support.
State-coordinated	The national government coordinates third-party attackers such as by “suggesting” operational details.
State-ordered	The national government directs third-party proxies to conduct the operation on its behalf.
State-rogue-conducted	Out-of-control elements of cyber forces of the national government conduct the operation.
State-executed	The national government conducts the operation using cyber forces under their direct control
State-integrated	The national government conducts operations using integrated third-party proxies and government cyber forces.

Source: Healey (2012, p. 2)

Multiple of these APT groups operate around the globe. These groups are also known for using an array of different techniques such as *Obfuscation* or *False Flag Operations*, thereby hiding their identities and making the attribution of cyber-attacks so much harder.

Depending on the priorities and agenda of their respective governments, the mission set of state-sponsored actors usually encompasses a wide spectrum of cyber-operations including but not restricted to espionage against governments, organizations, and individuals, deterioration or crippling of critical infrastructure, manipulating public discourse through disinformation and propaganda; and enhancing the arsenal of cyber capabilities, weapons, and tactics to enable further illicit cyber activity. Some state-sponsored threat actors may also conduct financially motivated cyber-operations (Canadian Centre for Cyber Security, n. d.).

Russia

When it comes to cybercrime, Russia has turned into a global powerhouse (Kshetri, 2016). According to Kadlecová (2015), the proliferation of Russian-speaking cybercrime business over the past decade is a testament for this trend. The link between the Russian government and organized crime groups based upon presumed reciprocally beneficial relationships may constitute a contributing factor. The unstable socio-political circumstances in the post-Soviet Union era provided a favorable environment for the commencement of efficacious and potent cybercriminal undertakings.

According to Galeotti (2017), the emergence of criminals following the collapse of the former Soviet Union was not a result of transnational criminal behavior, but rather based upon the exploitation of formerly state-owned assets. In reference to Galeotti (2017), Dr. Louise Shelley, a Professor at Schar School of Policy and Government, George Mason University, highlights that organized crime became entrenched in Russian life and society with the collusion of organized criminals and corrupt government officials exerting significant influence on the global economic and political landscape (Shelly, 2018). This metamorphosis exemplifies a transition from prior fragmented market frameworks to the establishment of proficient criminal entities with centrally administered structures and strong ties into the government. Russian security services, according to the United States government, are known to leverage the activities of cybercriminals and to safeguard them from prosecution for personal gains (CISA, n. d.-c; U.S. Department of Defense, 2021).

Russian APT groups have demonstrated their extensive range of capabilities on a large scale, including the launch of the catastrophic 2017 NotPetya attack (see Chapter 4.2.2) and the interference in the various electoral processes across Europe and the United States (Blackwill

& Gordon, 2018; FBI, 2016; Jensen, 2017; NCSC, 2018). Their activities include compromising and infiltrating IT systems and networks, exfiltrating sensitive data, and crippling critical infrastructure. In addition, Russian operatives play a crucial part in disinformation campaigns and spreading propaganda to exert political influence and promote the Kremlin's agenda. The Russia-Ukraine conflict has ushered in a new era, characterized by information warfare using misinformation and deep fakes coupled with frequent cyber-attacks to cause disruption (Denić & Devetak, 2023; Przetacznik & Tarpova, 2022). This underscores the crucial role of cyberspace in geopolitical rivalries. The main Russian cyber-actors include the Federal Security Service (FSB), the Russian Foreign Intelligence Service (SVR), the Russian General Staff Main Intelligence Directorate (GRU), and the Russian Ministry of Defense (ACSC, 2022, p. 33). The United States government attributes activities against critical infrastructure entities, and the private sector to the Russian SVR (CISA, 2021a). When it comes to illegal cyber-operations, the demarcation lines in Russia tend to be fluent. Besides the "official" actors within the intelligence community, there are various APT groups that complement the threat landscape. Among these groups, *Fancy Bear* (otherwise known as APT28) is a household-name when it comes to Russian APT groups, assumed to be associated with the GRU. Another notorious APT group is *Cozy Bear* (also known as APT29), which is believed to be linked to the FSB (Galeotti, 2017, p. 6). Poland's Military Counterintelligence Service has linked APT29 to continued cyber-operations against NATO and European Union countries (SOC Radar, 2023).

Iran

Static Kitten (otherwise known as *MuddyWater*) is one of Iran's prime APT groups, spearheading the regime's cyber-operations against government and private organizations across multiple sectors, including telecommunications, defense, local government, and oil and gas, across Asia, Africa, Europe, and North America. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Cyber Command National Cyber Mission Force (CNMF) and the United Kingdom's National Cyber Security Center (NCSC) link the group with cyber espionage and other malicious cyber-operations (CISA, n. d.-a). It is assumed that Static Kitten is a subordinate element within the Iranian Ministry of Intelligence and Security (MOIS) (U.S. Cyber Command, 2022).

In 2012, a cyber-attack hitting Saudi Aramco, the world's largest oil company, created global headlines. While a group named "Cutting Sword of Justice" claimed responsibility, strong evidence is pointing toward the Iranian government for being responsible for the attack

(Harknett & Smeets, 2022). While cyber-operations have thus far mainly targeted the Middle East region, there have been noticeable attacks against surrounding nations and beyond, including targets in India, South Asia, and the United States (CFR, n. d.-a; Fraunhofer, n. d.-c).

Iranian APT groups are known for carrying out disinformation campaigns and spreading propaganda to undermine election processes by discomforting voters. This includes setting up fictious media websites and spoofing legitimate ones about alleged voter suppression and other misleading information (otherwise known as *fake news*) to advance the regime's anti-American agenda (CISA, 2020; FBI, 2020).

To strengthen their cyber capabilities, Iran entered into a cooperation agreement with Russia in January 2021, aiming at establishing technology transfer, combined training as well as fostering cyber-security cooperation between both countries. Due to ongoing protests and public criticism against the Iranian regime, the internet has been the bone of contention and annoyance for the Iranian government. Geard toward tracing dissidents, suppressing opposition, and hindering the Iranian people to exercise their right of freedom of speech, the Iranian regime is actively cooperating with Chia to achieve tighter internet surveillance and censorship (Esfandiari, 2020; Khorrami, 2022; U.S. Department of Health and Human Services, 2022).

China

The Chinese Communist Party (CCP) is pursuing a whole-of-government effort to manifest its global influence and wants to turn the nation into a "cyber powerhouse" (Cary, 2021). As geopolitical tensions in the Asia Pacific (APAC) region and beyond are rising, China leverages an arsenal of APT groups as a force multiplier in the cyber realm. This encompasses diverse types, scales, motivations, and objectives (Kshetri, 2013). China's state-sponsored actors not only operate extensively in East Asia and the Western Pacific, which China perceives as its natural sphere of influence, but they also have a global presence across Europe, North and South America, Africa, the Middle East, and the Asia Pacific region. (CFR, 2022; ENISA, 2023). To do so, the Chinese government heavily invests into building and enhancing cyber capabilities including the establishment of a dedicated cyber-security military school. The inaugural batch of 1,300 students successfully completed their studies in 2022, marking a significant milestone. The CCP policymakers envision a yearly output of 2,500 graduates from this institution (Cary, 2021). Chinese military strategists recognize the paramount importance of cyber-operations within interconnected networks. Simultaneously, there has been a significant increase in cyber-attacks carried out by the Chinese government on foreign critical national infrastructure networks (ibid.). These attacks are highly sophisticated and have managed to evade detection even after the initial compromise, resulting in a joint warning being issued by government agencies in the United States, Australia, Canada, and New Zealand (NCSC, 2023).

Much like Russia, China leverages non-state actors too (Chen & Abu-Nimeh, 2011), including organized criminal groups and oligarchs, as proxies to exude hybrid influence, creating networks of power to exploit global spaces and flows (Sullivan, 2023). A group of threat intelligence researchers has identified almost 100 different APT groups operating from China with some of them having "enormous range" (Harknett & Smeets, 2022). Researchers have estimated that as many as 400,000 Chinese individuals are involved into organized cybercrime (Nobles et al., 2023). Some of these APT groups, such as APT 41, for example, frequently compromise codesigning while carrying out sophisticated software supply chain attacks against the United States and other countries (NIST, 2021). For China, cyber-operations are meanwhile part of the "new normal", and it is assumed, that there will be spillovers from the cyberspace into the conventional sphere (Maness & Valeriano, 2016, p. 49). Even though not every APT group act on behalf of the Chinese Communist Party (CCP), China's APT network is widely intertwined with the government and in possession of substantial cyber capabilities (Rosengren, 2023). These different China-based actors include *GreedyTaotie* (otherwise known as APT27), who has been made responsible for cyber-operations targeting foreign embassies for information theft on government, defense, and technology sectors (Arghire, 2023; U.S. Director of National Intelligence, 2021). Other prominent Chinese state-backed APT groups include *Red Apollo* (also referred to as APT10 or TA410) and *Zirconium* (otherwise known as APT31). Both specialize mainly in clandestine espionage operations. *Red Apollo* has been targeting foreign governments and officials. Conversely, *Zirconium* has put more emphasis on the ICT space (CFR, n. d.-b; Fraunhofer, n. d.-a).

North Korea

The North Korean government, officially referred to as the Democratic People's Republic of Korea (DPRK), runs extensive cyber-operations to gather intelligence, conduct attacks, and produce revenue. Numbers about North Korea's hackers vary depending on the source. Some estimate the number to be between 3,000-6,000 (Chanlett-Avery et al., 2017), while others estimate the number rather to be at around 7,000 (Ji-Young, 2019; Martin, 2018). These cyber warriors conduct a wide range of activities including theft, distributed denial of service (DDoS), espionage and sabotage (Martin, 2018). All this is aimed at enhancing North Korea's asymmetric military power by fortifying their cyber capabilities while minimizing internet dependency in the country. China has become a close ally and exchange partner for military training. Some 50 to 60 elite soldiers are being send abroad each year to study computer science, who later return to North Korea to perform cyber-attacks for the regime's military units (Ji-Young, 2019). Relative to the size of the population let alone the country's backwardness, and poor and antiquated infrastructure, North Korea commands a remarkably powerful and one of the largest cyber forces in the world. Estimates are, that North Korea has supposedly an additional 12,000 highly skilled civilian hackers as well as another 10,000 North Korean hackers who operate criminal activities remotely from China at their disposal (Kshetri, 2014).

According to the U.S. government, *"North Korea's malicious cyber activity is a key revenue generator for the regime, from the theft of fiat currency at conventional financial institutions to cyber intrusions targeting cryptocurrency exchanges"* (U.S. Department of the Treasury, 2020a). The capabilities are spread across multiple actors. The Reconnaissance General Bureau (RGB) is North Korea's premier intelligence agency that runs most of the regime's cyber-operations. Another key actor is the General Staff Department (GSD), which is responsible for military units and operations including conventional cyber-operations. It is assumed that unlike RGB, GSD is tasked with less offensive action.[38] Despite being heavily sanctioned over many years, North Korea has gained excellence in the cyberspace, making their operations a low cost, and low risk, yet highly rewarding undertaking (Andrew et al., 2015; Chanlett-Avery et al., 2017; Ji-Young, 2019; Kim, 2022).

Unlike some of their international counterparts, North Korean APT groups (such as *Lazarus Group* or *Hidden Cobra*, for instance) tasked to conduct heists in the cybersphere to aid the North Korean regime. Infamous for their sophisticated capabilities, there have been numerous examples, whereby North Korean threat actors have carried out strikes at an unprecedented scale to rack in large sums of money (CISA, n. d.-b; Davies & Chipolina, 2022). In 2019, the UN Security Council estimated, North Korea had attempted to steal as much as US$2 billion to subsidize its illicit ballistic missile and nuclear programs (U.S. Department of the Treasury, 2020a). North Korea has also been made responsible for creating and circulating the WannaCry ransomware in 2017 (see Chapter 4.2.1).

The FBI confirmed that *Lazarus*, one of the North Korean APT groups, was responsible for the theft of cryptocurrencies worth US$100 million from Harmony Horizon in 2022 (FBI, 2023). Yet, this was just one out of several lucrative cyber-operations conducted by

[38] For further research on the organizational setup of the North Korean government's cyber-operations, see e.g., Ji-Young et al. (2019) and Jun et al. (2015).

the regime that year. According to blockchain analyst firm Chainalysis, North Korea's cryptocurrency theft operations yielded a record-setting US$1.7 billion in 2022 only. This represents a four-fold increase compared to the US$429 million stolen by the regime in 2021 (Ng, 2023).

In June 2023, another case created headlines, when supposedly hackers from North Korea stroke again and stole at least US$35 million from an Estonia-based cryptocurrency platform (Lillis & Lyngaas, 2021). It is not a coincidence that North Korean hackers zero in on cryptocurrencies. Cryptocurrencies are vulnerable since decentralized finance (DeFi) protocols are vulnerable and lack regulation, making tracing the flow of funds impenetrable. It has also proved to be powerful vehicle for evading sanctions, as transactions are completed through encrypted transfers and not exchanged via commercial banks (Gramer & Iyengar, 2023). Despite being heavily sanctioned over years, North Korea continues to leverage their cyber-heists as an effective source of income to subsidize the "Kim dynasty" and their various weapons programs (CFR, n. d.-d; United Nations Security Council, 2019).

Western Cyber Actors

Although well-known and infamous APT groups are typically associated with Russia, China, Iran and North Korea, the United States, and the Anglo-Saxon intelligence community collectively (otherwise known as the *Five Eyes*), are certainly not lagging with respect to their offensive cyber capabilities.[39] In general, with the Central Intelligence Agency (CIA) and the National Security Agency (NSA) and other units at their disposal, the United Sates is considered to possess one of the most extensive, most sophisticated, and well-funded intelligence and cyber capabilities. For example, the United States government has conducted cyber-operations sought to disrupt, deny, degrade, or destroy and publicly acknowledged "waging a cyberwar" against the Islamic State, Iran, and North Korea (Harknett & Smeets, 2022). Supposedly one of the first offensive cyber-operations successfully launched against critical infrastructure was conducted by the United Sates and Israel, when infiltrating the network of an Iranian nuclear enrichment facility sometime before 2010 with a malicious worm named *Stuxnet*, but both governments have never acknowledged responsibility (Chen & Abu-Nimeh, 2011; Glenny, 2023; Mueller & Yadegari, 2012).

[39] The term "*Five Eyes"* refers to an Anglo-Saxon intelligence alliance between the United States, the United Kingdom, Canada, Australia, and New Zealand.

In 2021, the U.S. Cyber Command conducted a counterstrike against a ransomware group, supposedly *REvil* (see Chapter 4.3.6), and individuals supporting and funding ransomware operatives without disclosing details of the operation itself (Lillis & Lyngaas, 2021; Robinson, 2022). Besides the "official" intelligence agencies mentioned, other units including APT Groups are supposedly operating in the shadows about which little is known. *Equation Group* (otherwise known as *Tilded Team*, *EQGRP* or *G0020*), is such an APT group, for example (CFR, n. d.-c; Fraunhofer, n. d.-b). Following the September 11 attacks in 2001, huge efforts have been made, labeled as part of the *War on Terror* doctrine, to boost surveillance and data collection, among other things, in a systematic manner at an unprecedented order of magnitude. Numerous spy initiatives and programs have been run, partially with the self-concept that anything goes, with the public disclosures of whistleblower Edward Snowden, ultimately resulting in the so-called PRISM scandal which sparked international outcry (Denić & Devetak, 2023). The leaked material brought to light the existence of a mass surveillance program aimed at analyzing data from a range of internet services and technology giants, such as Google, Microsoft, Apple, Facebook, and others. Part of the PRISM program included the United States' interception of telephone calls, text messages, and chat messages of senior officials of their Western allies in Sweden, Norway, France, and Germany (Reuters, 2021).

4.3.8 Cyber-Terrorism

The term *cyber-terrorism* was coined by Barry Collin in the 1980s when referring to the convergence of the physical world and terrorism (Emery, 2005; Pollitt, 1997; Yunos et al., 2014), and further substantiated by Denning (2000) as follows:

> *"Cyber-terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."*

In a shorter yet similar direction, Lewis (2002) defines cyber-terrorism as *"the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."* From today's point of view, both definitions mentioned must be taken with caution and described as at least incomplete. However, both definitions were made in a different era, while cyber-terrorism has since evolved. Meanwhile, the cyberspace can be misused by terrorist groups in many ways. Besides using the cyberspace to strike an attack, terrorist groups heavily rely on the internet as a vehicle for intra-group communications, recruiting, fund-raising and dispersion of propaganda (Denić & Devetak, 2023; Weimann, 2016).

In summary, cyber-terrorism remains a relatively broad term with some arguing in favor of a narrower definition relating to disrupting critical infrastructure and creating panic and unrest, while others suggest a wider definition relating to cybercrime, spreading propaganda, and recruiting followers. In any case, the term cyber-terrorism should not be confused as synonymous with cybercrime since the motive of the perpetrators, their actions, and the scale of their actions vary. Put simply, cyber-terrorism can be viewed as *"using computer technology to engage in terrorist activity"* (Brenner, 2007). According to International Humanitarian Law (IHL) including the Geneva Convention, military action is not supposed to target civilian infrastructure as it would otherwise constitute war crimes. Terrorists, however, do not adhere to these principles. They recklessly harm, coerce, and demoralize civilian population, thereby undermining society's ability to maintain order (Brenner, 2007). Their motives are primarily of religious, ideological, or political nature but may include financial gain as well (Gable, 2010).

While there is undoubtably the risk of a terrorist group (e.g., Al-Qaida or ISIS) engaging in large-scale cyber-attacks, thus far, terrorists tend to play a minor role when it comes to cyber-attacks relative to the other groups of threat actors. Although conventional terrorist organizations might be motivated to carry out a destructive cyber-attack leading to the loss of life or substantial damage, they do not possess the capacity to do so. From today's perspective, only a hostile nation-state could do that (Buckland et al., 2015; Jayakumar, 2021; Weimann, 2004). Besides using the internet for spreading propaganda and recruiting new members, it appears far more likely that terrorists use the cybersphere to do fundraising and commit financial crime (e.g., money laundering) to subsidize their real-world activities. The emergence of the Cybercrime-as-a-Service model (see Chapter 3.3.3) might however, at least to some extent, help terrorists to overcome their limitations since it allows even individuals or groups with no hacking skills to hire a professional hacker instead. Yet, many of the off-the-shelf cyber-attack services offered on the Dark Web (e.g., smaller DDoS attacks) for sale, lack sophistication. Unless plotted into a complex cyber-operation across multiple attack vectors, basic attacks are not too hard to thwart off. At least from today's perspective, the prospect of a terrorist remotely hiring a cybercriminal to conduct a cyber-operation on a level and scale of an ATP group, appears to be a too far-fetched of a scenario.

4.4 The Infrastructure Enabling or Supporting Threat Actors (Extract)

Cybercriminals rely upon technology like everybody else. Threat actors employ a range of technological resources, encompassing both rudimentary and sophisticated tools, such as artificial intelligence (AI) tools, automated software creation tools, and specialized exploits. Additionally, they utilize tools for identifying potential targets and locating vulnerabilities within systems (Alnifie & Kim, 2023). Not only are cybercriminals exposed to cyber-threats themselves, but they are also confronted with the constant threat of seizure through law enforcement (Kropotov et al., 2020a). Their operations are therefore underpinned by operational security to obscure their identities, secure communication channels leveraging encryption, and disguising financial transactions. In turn, all these support functions create a huge opportunity for the expansion of the so-called gray infrastructure, which enables and fuels the crime-as-a-service industry (Europol, 2022, p. 16). These vendors indirectly benefit from the "goldrush" in the Dark Web by metaphorically selling the shovels and other equipment to criminals to facilitate their illegal activity.[40]

The availability of such gray infrastructure increases the operational security of criminals with Russia and China providing a safe haven for many of the questionable companies operating in the shadows (Richardson & North, 2017). Other services can be classified as operating in the "gray zone", or in other words being on the verge of legality. Shielded from the public, ICT services of this kind are promoted in underground forums and usually located in countries with stringent data protection laws or countries that lack strong international ties and are not known for collaborating with foreign authorities or simply lack the capabilities and resources to do so (Europol, 2022, p. 35; Kropotov et al., 2020a). Among other things, services in the so-called gray zone encompass bulletproof hosting providers, down-and-dirty cryptocurrency exchanges, and VPN services that provide refuge for criminals. Irrespective of the service in question, strong end-to-end encryption is always an important design criterion to

[40] This intersects with cybercrime-as-a-service (CaaS) offerings, playing a crucial role in illegal value chains (see Chapters 3.3.3 and 3.3.4 respectively).

elude prosecution (Europol, 2022, p. 18). Also, vendors may now be aware of law enforcement's tactics and therefore take steps to protect themselves (Europol, 2022, p. 35).

4.4.1 Internet Overlay Networks

The Deep Web encompasses all websites that have not been indexed by search engines and are mostly used for everyday tasks. On the other hand, the Dark Web is a subset of the deep web intentionally made invisible. To access these hidden parts, an overlay network is necessary. This overlay network is a conceptual layer that operates on top of a network through the application of virtualization technology. One of the most common ones is The Onion Router (Tor). Designed to increase privacy and anonymity and conceal interaction, Tor is the most known vehicle to access the Dark Web and thus regularly used by bad actors to disguise their identity and location. This includes even conspiracy theorists, extremists, and terrorist groups that share their propaganda, thereby elevating the Dark Web into a significant communication channel (Denić & Devetak, 2023). This is a real threat because many users take misinformation, as witnessed in the context of the COVID-19 pandemic, at face value and consider them more trustworthy than the content provided by the government which leads to a greater loss of authority and makes individuals and their social environment more susceptible to believing conspiracies (Topor & Shuker, 2020). While the Tor browser is often used synonymously with the Dark Web, not all users are automatically criminals or conspiracy theorists. The browser can also be used to access the regular internet. Additionally, it is utilized by a variety of legitimate users who wish to protect their privacy. This includes investigative journalists, politicians, activists, and opposition members, particularly those operating under repressive regimes where their activities would otherwise be hindered or sanctioned (Denić & Devetak, 2023; Weimann, 2018).[41] Especially in countries where freedom of speech and other human rights are heavily restricted, and minorities are oppressed or persecuted, these individuals often have no other choice but to communicate through channels that offer a higher level of confidentiality. Certain countries make attempts to completely restrict the utilization of Tor and consider its usage as unlawful due to its ability to impede internet censorship and hinder user

[41] While the public Internet provides some level of pseudonymization and security for all users, it has seen a noticeable decrease accelerated from 2001 onward following the proclamation of the global war on terror. Increasingly so, nation states have exercised control and surveillance towards the cyber domain. The first example of a government surveilling Internet activity is the Russian Federation, having established control over all electronic communication back in 1996 (cf. Denic & Devetak, 2023).

tracking. This holds especially true for nations that commonly exert stringent governmental control and engage in extensive technical surveillance.[42] Nonetheless, in most jurisdictions, downloading and using the Tor browser is generally not illegal. Rather, it is the engagement in illegal activities conducted through the browser that typically constitutes a criminal offense.

Despite its common association with illicit activities, not all content on the Dark Web is illegal either. In fact, a 2016 study by research firm Terbium Labs examining 400 randomly chosen .onion[43] sites concluded that more than half of all domains on the Dark Web were indeed legal (Kumar, 2019). Based on a much larger sample size, Moore and Rid (2016) came to similar findings. Out of the 5,205 .onion websites that underwent scrutiny, it was discovered that 1,547 of them (57%) contained illicit content, including all sorts of pornography, illicit finances, drug hubs, weapons trafficking, counterfeit currency, and terrorist communication. This leaves the remaining 43% of the websites with legal content. The results suggest that the websites on Tor hidden services are mostly used for criminal activity. An interesting observation is the near-absence of Islamic extremism at the time of the study, suggesting that the *"darknet's propaganda reach is starkly limited,"* thus these groups would be more inclined to use the regular internet instead.[44] As per their findings, the single largest category of illicit websites (27%) was drug-related, comprising both pharmaceutical products and illegal substances. A multitude of vendors exist, ranging from regional marketplaces to single-page vendors promoting a selection of their self-manufactured products. The range of substances available for purchase on the Dark Web is quite extensive, catering to different markets with specific preferences. These substances encompass cocaine, marijuana, methamphetamines, and various types of acid. Additionally, the Dark Web serves more discerning markets, such as those

[42] Examples include Burma (otherwise referred to as Myanmar), China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, and Vietnam (see Buckland et al., 2015, p. 21).

[43] A URL ending with .onion indicates a hidden top level domain in the anonymization service Tor.

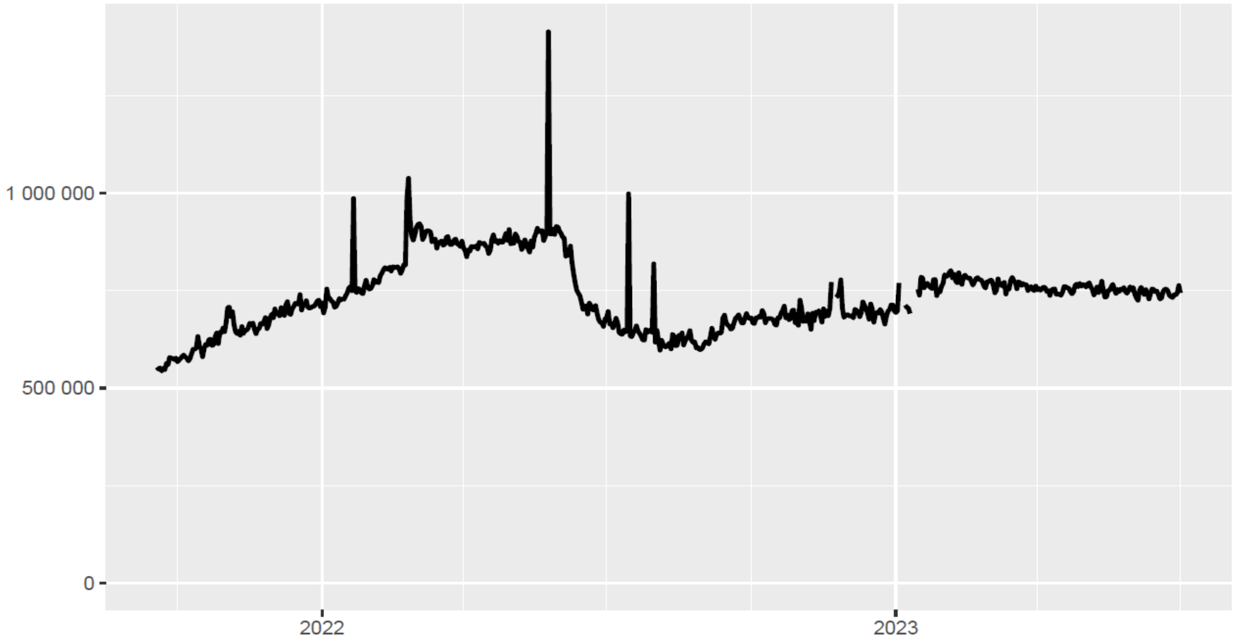
[44] This statement contrasts with Denic & Devetak (2023), Morre & Rid (2016) and Weimann (2016, 2018), who argue that Islamic State heavily utilized the Dark Web following the 2015 attacks in Paris to avoid censorship, spread propaganda, conduct fundraising campaigns and anonymously facilitate the transfer of funds. Furthermore, as pointed out by Topor & Shuker (2020) and Denic & Devetak (2023), along with the emergence of the COVID-19 pandemic, evidence suggests that user behavior across the board changed with an increasing number of people accessing the Dark Web instead of relying on established media websites and regular websites on the internet to seek and exchange information. Moore & Rid (2016) might reflect a different *zeitgeist*. Future research should consider the potential change in user behavior over time when it comes to sharing propaganda on the Dark Web and thus cross-validate previous results.

involved in the trading of anabolic steroids and Viagra-type medication. These substances make up a significant portion of unlawful activities on the Dark Web.

The second largest category of illegal activities on the Dark Web, making up 21% of the total, involves illegal financial services such as money laundering, trading illegally obtained or cloned credit cards, stolen accounts, and counterfeit currency. This underscores the prominence of financial crimes within the Dark Web. Interestingly, extremism—including terrorism, militancy, and propaganda—accounts for only 9% of all illegal .onion websites. In contrast, just 6% of the illegal websites were linked to “hacking,” specifically the sale of malware or DDoS-for-hire services. These findings indicate that communities focused on drugs or illegal financial services are significantly larger, with about four times the number of illegal websites and forums compared to traditional cybercrime activities. Despite the criminal activity on the Dark Web, it is important to note that Tor is widely used for lawful purposes. Research by Moore and Rid (2016) found that only 3% to 6% of Tor traffic is associated with hidden .onion websites, while over 90% of Tor traffic is directed toward regular internet sites. Legal .onion websites include newspapers, blogs, search engines, and even Facebook, offering users enhanced privacy. As of 2023, there were approximately 750,000 websites on the Tor network and around 50,000 downloads of the Tor browser per day, highlighting the network’s significant legitimate use for privacy and security, far beyond illegal activities..

In recent years, there have been numerous spikes in the in the number of .onion websites (see Figure 12).

Figure 12: Unique .onion v3 Addresses



Source: Tor (n. d.)

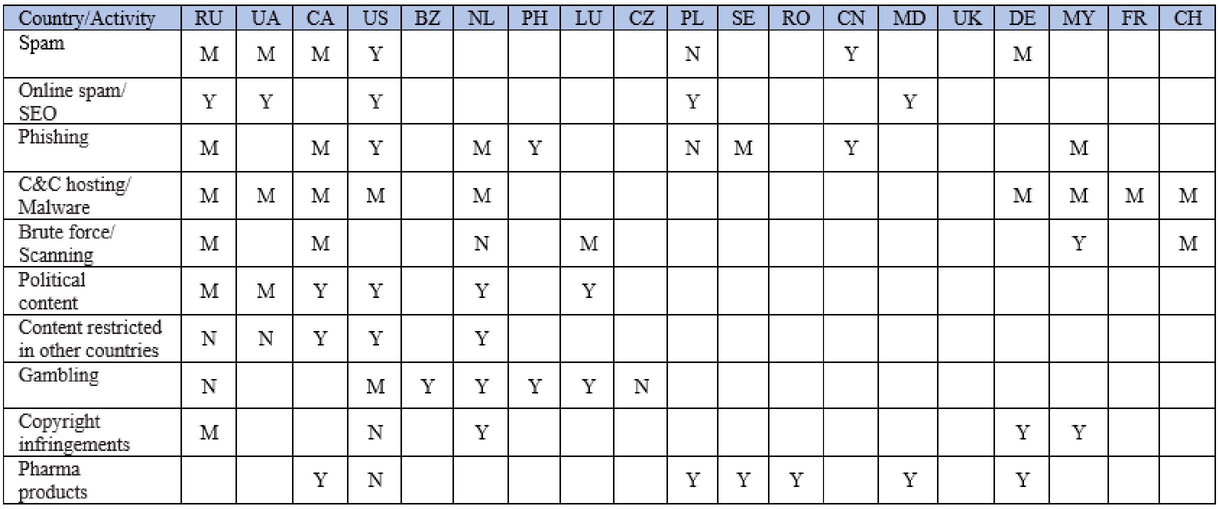
For instance, a similar phenomenon occurred in 2016, as observed by a scholar at the University of Surrey and reported by the BBC (Baraniuk, 2016). However, there is still speculation as to what exactly caused the jump, which is warranting further research in this area. For the sake of completion, though it is perhaps the most known one, Tor is by far not the only such overlay network. Other examples include Freenet, I2P, and private community networks such as Open Mesh, Guifi, and Freifunk (Kropotov et al., 2020a). The Deep Web is hard to measure due to hidden or restricted data. Approximations suggest that the Deep Web surpasses the size of the regular internet by a staggering 400-500 times (Weimann, 2016). Notably, Google's indexing capabilities are limited to a mere 16% of the internet, rendering it incapable of accessing any content within the Deep Web. Any search only yields 0.03% of the total information available online (ibid). This turns the regular internet into the tip of the iceberg (Weimann, 2018).

4.4.2 Bulletproof Hosting

Cybercriminals utilize various tactics to protect their illegal activities, and one method involves hiring *bulletproof* hosters who pose as legitimate businesses to hide their true intentions. These hosters customize their services to meet the specific needs of the criminals they serve. The term "bulletproof" suggests that these hosters have highly resilient infrastructure that is shielded from legal actions, often by operating from offshore locations and using advanced technologies to conceal identities. These bulletproof hosting services are essential to keep the underground economy afloat (Huang & Madnick, 2017), with prices starting at around US$300 per month (Akyazi et al., 2021). A prominent characteristic of these services is their robust end-to-end encryption, which ensures that messaging application providers cannot reveal the content of communications, even in response to legal subpoenas (Europol, 2022). While these providers may seem like ordinary internet service providers or hosting companies, they often offer additional services that fall into a morally ambiguous gray area. The level of criminality associated with these services depends on the provider and the jurisdiction in which they are based. However, after finding enough evidence of criminal abuse, law enforcement agencies consider them to be criminal enterprises and go after the individuals involved (ibid.). Notable examples of such operations include the so-called "cyber bunkers" in Germany and The Netherlands, where former military bunkers the Cold War era were rented and transformed into data centers for hosting illegal services on the Dark Web. The advanced physical security measures at these sites further complicated efforts by law enforcement to conduct raids, providing significant protection for these operations. Their infrastructure, among other things, hosted *Wall Street Market*, one of the world's largest illicit marketplaces for drugs, hacking tools and cybercrime services; *Orange Chemicals*, a website trading synthetic drugs; or *Cannabis Road*, a drug-dealing marketplace (Caesar, 2020; Moulson, 2019).

Research by Alrwais et al. (2017) show that lower-tier hosting providers have simplified the process of becoming a reseller, often requiring minimal verification. For example, one provider confirmed authenticity via text, while another required a phone call that functioned more as a sales pitch than true authentication, making it easy for criminals to quickly sign up while concealing their identity. According to Kropotov et al. (2020a), relative to cybercrime and related activities, legislation varies by region with some countries being more progressive and stringent while others tend to be laxer in some respects. Like legitimate enterprises, organized crime syndicates also engage in "strategic decision-making" processes to expand their operations and increase the scale of business. They carefully assess various factors such as the social, political, and legal environment when determining the best destination to establish their operations. By analyzing these elements, criminal organizations aim to optimize their chances of success and minimize potential risks associated with their illicit activities. As such, depending on the nature of the service in question, some countries appear to be a more attractive location of choice than others (see Table 8).

Table 8: Preferred Criminal Hosting Locations by Country and Activity[45]



Country/Activity	RU	UA	CA	US	BZ	NL	PH	LU	CZ	PL	SE	RO	CN	MD	UK	DE	MY	FR	CH
Spam	M	M	M	Y						N			Y			M			
Online spam/ SEO	Y	Y		Y						Y				Y					
Phishing	M		M	Y		M	Y			N	M		Y				M		
C&C hosting/ Malware	M	M	M	M		M										M	M	M	M
Brute force/ Scanning	M		M			N		M									Y		M
Political content	M	M	Y	Y		Y		Y											
Content restricted in other countries	N	N	Y	Y		Y													
Gambling	N			M	Y	Y	Y	Y	N										
Copyright infringements	M			N		Y										Y	Y		
Pharma products			Y	N						Y	Y	Y		Y		Y			

M = Maybe Y = Yes N = No

Source: Kropotov et al. (2020a, p. 8)

[45] The respective countries in question have been abbreviated as follows: RU: Russia; UA: Ukraine; CA: Canada; US: USA; BZ: Brazil; NL: The Netherlands; PH: Philippines; LU: Luxembourg; CZ: Czech Republic; PL: Poland; SE: Sweden; RO: Romania; CN: China; MD: Moldovia; UK: United Kingdom; DE: Germany; MY: Malaysia; FR: France; CH: Switzerland

For example, as suggested by Kropotov et al. (2020a), Switzerland and the Netherlands are discussed in underground forums as suitable locations for setting up shell companies to proxy hosting operations. China, on the other hand, may be of interest because many activities are legal that are prohibited in other countries. Russia is very stringent with respect to pornographic or political content but seems to be a more permissive jurisdiction when it comes to malicious [cyber] activity if it does not target domestic users. Seychelles, Belize, the Dominican Republic, and Panama are deemed popular in underground discussions for having an attractive combination of good internet connectivity coupled with slow responses to cyber-threats for various reasons, which turns them into a save heaven for cybercriminals (ibid.).

4.4.3 Botnets

Sometimes referred to as a zombie, a bot is an internet-facing device that is compromised with malware. A botnet is an entire army of such infected computers or IoT devices that can be remotely controlled and used to send spam, distribute malware, or perform DDoS attacks—all without the owners' knowledge (Canadian Centre for Cyber Security, n. d.).

IoT devices (think smartwatches, wearables, etc.) have enjoyed huge popularity in recent years but many of these devices are insufficiently protected. As emphasized in Chapter 1, the proliferation of these devices continues to surge annually, culminating in a total that now exceeds more than 10 billion. Although it is not possible to determine the exact number of bots in a botnet, estimates for the total number of bots in a complex botnet range from a few thousand to over a million (see Chapter 3.3.3). Cybercriminals are monetizing these botnets by offering them for rent or reselling them to perform various criminal actions.

4.4.4 DDoS Protection

It might sound surreal, but distributed denial-of-service (DDoS) attacks are so widespread that they plague criminals, too. Bad actors compete against one another just like legitimate businesses and have no scruples with leveraging cyber-attacks to take a competitor out of business. Also, a disgruntled or banned member of an underground forum who left in bad standing might procure a DDoS attack to take the forum offline. A downtime could impede the forum's reputation as it would question the forum's stability and get members to leave. Even DDoS extortion (RDDoS) can be observed, whereby the provider of an underground community or underground shop is requested to make a ransom payment in order not to be taken offline. Making matters worse, unlike a legitimate business, the provider of such an illicit forum or shop cannot file a complaint and contact the authorities as he would most probably expose himself to prosecution, too, because of his dubious source of income. It is, therefore, commonplace that bulletproof hosting providers offer DDoS protection to safeguard their questionable clientele (Europol, 2022; Kropotov et al., 2020a, 2020b).

4.4.5 Cryptocurrencies and Crypto Wallets

Because of their anonymous nature, cryptocurrencies are the de facto standard when it comes to facilitating illegal transactions in the Dark Web. That way, in the absence of a bank acting as the intermediary, criminals can camouflage and launder their illegal funds in the shadows (Denić & Devetak, 2023). The association between Bitcoin and illicit activities is well-documented, as an estimated 25% of its users are believed to engage in unlawful practices. Estimates are that the staggering amount of US$76 billion worth of illegal transactions is facilitated that way (Foley et al., 2019). However, as legitimate cryptocurrency exchanges have elevated their know-your-customer (KYC) guidelines and regulations, it is becoming harder for criminals to shield their identities (Europol, 2022, pp. 11-18). To stay under the radar, cybercriminals are increasingly moving away from Bitcoin toward other cryptocurrencies such as privacy coin Monero (Denić & Devetak, 2023; Europol, 2022, p. 36). Monero uses a blockchain with privacy-enhancing technologies to obfuscate transactions to achieve anonymity and fungibility. As a result, it is not possible to decipher addresses trading Monero, transactions, balances, or histories (Denić & Devetak, 2023). Due to the popularity among cybercriminals, including some of the most notorious ransomware gangs, Monero has attracted controversy since its inception. For the authorities, in turn, this is a thorn in the side. The United States Internal Revenue Service (IRS) has offered a bounty of US$600,000 to anyone who succeeds in decoding transactions made via Monero or Lightning coins (Murphy, 2021).

4.4.6 VPN Services

As with the rest of the population, cybercriminals also opt for VPN services to ensure the protection of their communication and to shield their internet browsing (Europol, 2022, p. 18). Nevertheless, there exists a significant disparity in their preferences. Certain actors gravitate towards mainstream commercial products, whereas others choose to exclusively endorse niche VPN services that are primarily advertised in clandestine online communities. Alternatively, they may utilize specialized software tools like OpenVPN or SoftEther.

Additionally, certain actors adopt a business model centered around providing anonymizing services for hire (Kropotov et al., 2020b, p. 24).

4.4.7 Other Services

The pervious sections provide an extract. There are many other product categories and illegal services available to fuel the underground economy. This, among other things, include Money-Laundering-as-a-Service (MLaaS), which runs “dirty” money through processes to make it look legitimate; Reputation-as-a-Service (RaaS), which allows fraudsters to make their offerings appear more trustworthy due to faked user ratings; Phishing-as-a-Service; Hacker-Training-as-a-Service (HTaaS), which—as the name already suggests—allows novel criminals to hone their skills based upon additional training that can be purchased; and so forth. The “as-a-service” category is almost endless. Going through all illicit goods and service categories would go well beyond the scope of this thesis.[46]

[46] For further reading about the illicit cybercrime-as-a-service (CaaS) offerings and the respective infrastructure used by cybercrime actors see e.g., Manky (2013); Huang et al. (2017, 2018); Kropotov et al. (2020a, 2020b); Nobles et al. (2023). From a law enforcement perspective, see e.g., Europol (2022).

CHAPTER 5
CYBER-RISKS

5.1 Cyber-Risk Management

Cyber-risk pertains to the potential danger stemming from cyber-related incidents due to insufficient protection. This includes perils such as financial loss, disruption, or damage to an organization or its brand. Cyber-risk involves a comprehensive assessment of the exposure to security flaws in the context of internal and external threats, geared toward minimizing downtime, preventing data loss, and maximizing productivity. Wrede et al. (2020) define it as *"any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, integrity, or availability of data or services"*. However, the comprehension of cyber-risk presents a complex challenge that many organizations struggle with. The incorporation of a risk perspective further amplifies the complexity by encompassing the intricate interplay of technical, social, and economic factors (Böhme et al., 2020; Fielder et al., 2018).

As illustrated by Böhme et al. (2020), a single microchip in a piece of hardware has the capability to perform a number of computational operations that *"exceeds the number of atoms in the known universe"*. Similarly, software may consist of several million lines of code. All these factors provide ample opportunity to spot potential vulnerabilities. Common programming mistakes enable cyber-threat actors to manipulate the logic and engage in malicious activities (ibid.). In turn, the likelihood of flaws or loopholes being overlooked is disproportionately surging. With the current technological means available, it appears virtually impossible to thoroughly examine all aspects in their entirety in advance. For most organizations, realistically it is therefore no longer a question of whether they get hit by a cyber-attack; it is just a matter of time. As such, cyber-risk has emerged as one of the most pressing business risks in the 21st century, effecting organizations around the globe (WEF, 2023b; Wrede et al., 2020). Hence, it is imperative for organizations to possess effective capabilities for evaluating the potential hazards, understanding the weaknesses, and identifying viable remedies prior to threat actors capitalizing on them (Lahcen et al., 2018). One of the particularities of cyber-security is that it is intricately linked with various other types of risks that organizations face. To that end, cyber-risk forms an integral part of Enterprise Risk Management.[47] Nonetheless, research indicates that cyber-risks are still taken rather lightly. While a board of directors' survey shows that board members are increasingly more cognizant of the importance of cyber-security with 88% seeing it as a business risk, only 12% have a dedicated board-level cyber-security committee to address these concerns (Gartner, 2022). This absence of action may be due to a lack of understanding, resources, or leadership. However, boards must take decisive action to minimize risks and protect against cyber-attacks and there is a significant amount of space for improvement. Of 1,500 corporate directors polled by McKinsey & Company, a scant 7% of the participants perceive their boards to have excelled in risk management in the previous year (Aufreiter et al., 2022). In a separate study, based upon more than 1,000 executives (n = 1,312) polled, roughly one-third (34%) reported that their organization had no method to measure or express cyber-risks (Marsh/Microsoft, 2018). This may in part be attributed to the absence of reliable and publicly accepted sources of information, making it difficult to estimate the economic magnitude of cyber-risk (Eling & Wirfs, 2016). The observation echoes the sentiment expressed by Peter Drucker, who famously stated, *"if you can't measure it, you can't manage it"*.[48] Against this background, it remains difficult to comprehend how organizations can go full steam ahead with the adoption of digital technology while keeping the radar switched off as it increases the odds of hitting an iceberg. As highlighted by Jalali et al. (2019), former White House Chief Information Officer (CIO) Theresa Payton stated, *"preparing, planning, and especially testing for a cyber incident is crucial for all companies, both large and small. Whether your company has been actively managing cyber-security risk for years or you are just beginning to develop an incident response capability, it is critical for boards and executives to engage employees in developing a robust, integrated approach to incident response. Unfortunately, companies too commonly put this task off and then find themselves flat-footed during a breach."*

Despite the availability of sufficient financial resources, investing in cyber-security initiatives is not a trivial task, as cyber-threats continue to evolve and create uncertainties

[47] Boyson (2013) refers to Enterprise Risk Management as *"A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

[48] Peter Ferdinand Drucker (1909-2005) was a renowned management consultant, educator, and author of Austrian American descent. His noteworthy contributions encompassed both the philosophical and practical aspects of modern management theory.

(Fielder et al., 2018). Therefore, effective cyber-risk management requires the removal of various obstacles that hinder the process. These obstacles go beyond technical aspects and comprise collaboration among different stakeholders, breaking down of silos, and promoting a better understanding of risks and responses to threats. Inadequately defined security incident crisis communication roles, responsibilities, and expectations can lead to role confusion, processing delays, and conflicting messaging. This lack of clarity can result in ineffective communication with staff, partners, suppliers, consumers, regulators, government officials, and the public. In the absence of a well-structured plan, messages may be unclear, untimely, or contradictory, further exacerbating the challenges faced during a security incident crisis (D'Hoinne, Watts, Olyaei, et al., 2022). A set of frameworks such as ISO/IEC 27005 or the NIST’s Risk Management Framework (RMF) exist, to help organizations operationalize their cyber-risk strategy (NIST, n. d.-b).

The financial impact of a cyber-attack can be devastating, and without proper insurance coverage, companies may struggle to recover from the damages. Therefore, there has been skyrocketing adoption of cyber insurance in recent years, which is widely perceived as a vehicle to transfer such risks (Böhme et al., 2020). However, while an insurance policy might represent one piece of the puzzle of a cyber-risk strategy, it is far from being a silver bullet that solves all problems under the sun. Cyber insurance policies frequently come with various restrictions that can limit the extent of coverage provided. This may include a maximum coverage amount for losses, such as US$10 million or US$100 million for example, depending on the specific policy and insurance provider (Eling & Wirfs, 2016). These policies also have exclusions, such as self-inflicted losses, accessing unsecure websites, terrorism, state-backed attacks, cyberwarfare, and more. Some policies also require a catalogue of security measures to be implemented for coverage. Additionally, there are indirect consequences of cyber losses, such as reputational damage, which are not typically covered by insurance. The dynamic nature of cyber-risk and the multitude of exclusions create uncertainty regarding the extent of coverage provided by cyber insurance policies. Furthermore, the lack of standardized terminology among insurance offerings makes it challenging to compare different policies (ibid.). It is essential to note that cyber insurance can also have adverse effects, such as *moral hazard* problems, where companies may reduce investments in self-protection due to the presence of insurance coverage, as well as biases like *optimism* or *overconfidence*, instigating riskier behavior after *externalizing* certain risks.

In the meantime, the insurance industry has recognized that cyber policies, initially hailed as a lucrative area for future growth, now pose a significant liability risk. This has led to a robust 28% year-over-year markup in cyber insurance premiums in response to the surge in cybercrime and its associated threats, including costly data breaches, ransomware attacks, and subsequent litigation (Violino, 2022). In certain instances, the yearly premiums that corporations are obligated to remit have even surged by up to 50%. The exacerbation of the turmoil is further compounded by the reality that hackers intentionally direct their efforts towards specific companies due to the presence of insurance coverage, assuming they are more likely to pay (Lerman & Vynck, 2021). As a result, insurance providers are cutting their coverage, which makes it difficult for some companies to afford or obtain cyber insurance policies (Violino, 2022). A global wave of cyber-attacks triggering immense insurance claims could quickly turn into a financial meltdown. The potential impact of just a few major incidents on large enterprises can eliminate the premium earnings of an entire year. Despite natural disasters causing claims in excess of US$100 billion for two consecutive years, the CEO of ZurichRe, one of Europe's largest insurance companies, has warned that cyber-attacks may simply become "uninsurable" due to the growing disruption they cause (Smith, 2022). AXA, another prominent European insurance company, has meanwhile officially announced to cease providing coverage for ransomware payments (Lerman & Vynck, 2021).

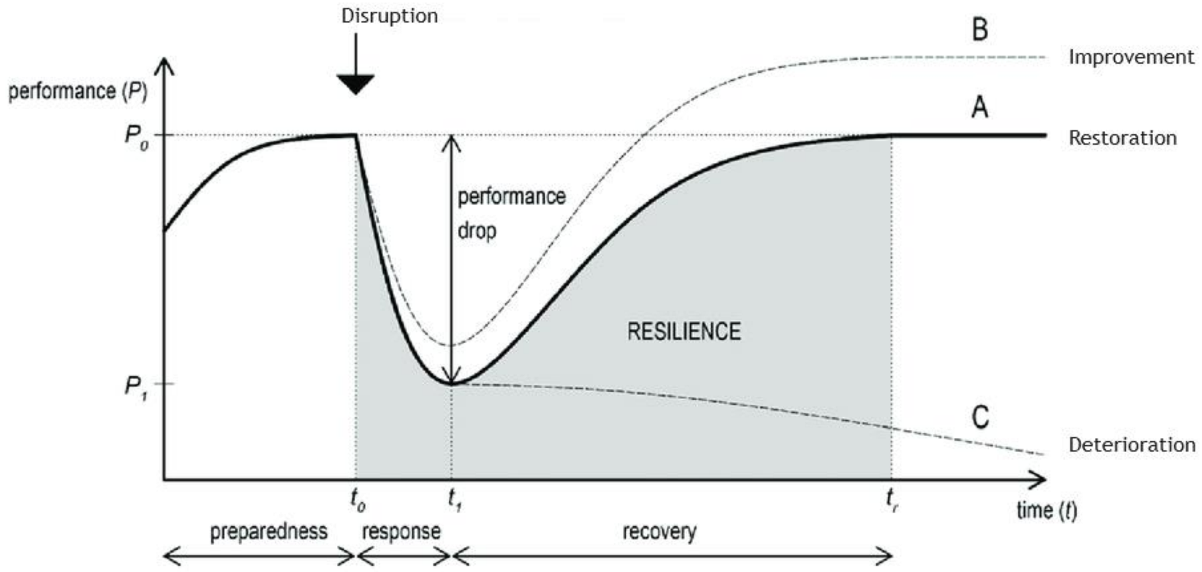
Therefore, it remains paramount for organizations to assess their cyber-security risks and take appropriate measures to protect themselves and their customers. Relying too heavily on insurance coverage in times of uncertainty may prove to be an unreliable and naive approach, which could potentially lead to grave ramifications.

5.2 Cyber Resilience

While cyber risk management deals with identifying and mitigating cyber-related risks to prevent an attack from happening, cyber resilience goes one step further and is geared toward the organization's ability to promptly restore business operations in the event of a successful attack. NIST (n. d.-a) defines cyber-resilience as *"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment".*

In the event of a successful cyber-attack, the house is literally on fire. When it comes to response and recovery, every minute counts. The ability to quickly contain the threat, regain control of the situation, and restore regular business operations is often referred to as *business continuity* and is crucial. This encompasses the strategic planning and implementation of measures to ensure the uninterrupted operation of a business or organization in the face of potential disruptions or crises. By prioritizing resilience and preparedness, businesses can enhance their ability to withstand and recover from adverse events, safeguarding their operations and minimizing potential losses (see Figure 13).

Figure 13: Cyber-Resilience Curve



Source: Adapted from Koren et al. (2017)

The previously mentioned depiction highlights three potential outcomes that typically occur after a business disruption: (A) the restoration of services, (B) an improvement resulting from a *postmortem* analysis and the application of "lessons learned", and (C) deterioration if the organization fails to recover fast enough and the hazardous event continues to unfold.

In line with this framework, empirical studies show that failing to quickly respond to a cyber-attack is no longer tolerable as it provides a gaping security loophole to threat actors. Adversaries will ruthlessly capitalize on any sizable time gap between the initiation of a cyber assault and its detection and response, providing them with ample time to steal data and inflict substantial damage. Study findings demonstrate that the preparation and execution of regular simulations, commonly referred to as "fire drills", can yield significant benefits. For instance, a recent study revealed that organizations with an incident response plan and a history of conducting simulations experienced an average cost reduction of US$2.66 million per incident compared to companies without such a plan and without testing (IBM/Ponemon Institute, 2022). The notable cost difference between the two groups, US$3.26 million and US$5.92 million, respectively, represents a reduction of 58%. Despite the evident advantages of practicing crisis management and preparing, only 63% of companies have taken such measures (ibid.). In a similar vein, a separate study revealed that organizations who give precedence to cyber investments encounter costs per cyber-security incident that are up to three times lower in comparison to their counterparts (Dal Cin et al., 2023). If empirical evidence demonstrates that is pays off taking precautions, one needs to wonder why organizations are hesitant to do it. One possible reason for this mismatch may be attributed to an *optimism bias* or *overconfidence*, whereby decision-makers believe that they or their organizations are not susceptible to a cyber-attack or that their capabilities are sufficient to render such plans and exercises unnecessary. Another explanation could be the existence of a *mental accounting bias* or *loss-aversion bias* in which individuals erroneously think it might be cheaper not to invest because the needed cyber-security investments exceed the costs of an incident. Although it might sound pragmatic and rational, people can be terribly wrong. All of this is perplexing considering the sheer facts. Unfortunately, affected companies often realize this only retrospectively after costly damages have already occurred, damages that could have either been avoided altogether or at least significantly limited in value.

For example, quite remarkably, Colonial Pipeline decided to hire its first Chief Information Security Officer (CISO) in 2022, only after encountering a cyber-security incident in the year prior, that knocked off the entire pipeline operations over several days, caused fuel shortages across large parts of the United States' East Coast and coerced U.S. President Joe Biden to declare a state of emergency (see Chapter 5.5.2 for further details) (Dal Cin et al., 2023). While this is just one example, it illustrates that cyber-security is still taken lightly even at large corporations and those operating in the critical infrastructure space. As a result, the United States government enacted new legislation and tighter regulatory requirements concerning the cyber-resilience as it relates to critical infrastructure (U.S. White House, 2021a). But again, this only happened after an embarrassing event that could have possibly been avoided. This anecdotal evidence is consistent with empirical studies. Although corporate boards should prioritize cyber-security, often they do not. Nearly six out of 10 CISOs (56%) concede that their cyber-security teams are either not consulted or are consulted belatedly when urgent strategic decisions are made by their organization's management board (EY, 2021). The underlying causes in this observation may also be attributed to the presence of cognitive biases and heuristics during the decision-making process, necessitating further investigations. Moreover, despite the demarcation lines between cyber-risk and cyber resilience, findings suggest that there is still widespread confusion about the terms among practitioners, even among professionals within the security realm. According to the WEF (2023a), 59% of cyber leaders say cyber-resilience and cyber-security are synonymous with the differences not well understood. Among those, over 90% of cyber leaders who consider cyber-security and cyber-resilience interchangeable also believe they are resilient. This is of concern as it may give decision-makers and organizations a deceptive sense of security. Without fully comprehending the scope of the exercise at hand, the downside is that the measures taken are insufficient or in other words a safety net has been put in place that is still full of loopholes. Again, this may only come to surface after the fact when it is already too late.

5.3 Digital Technology

The introductory section emphasizes the swift rate of change and growing interconnectivity of the world. This observation is reinforced by the proliferation of global technological trends that yield the potential to be of transformative nature. These developments encompass a wide range of areas such as cloud computing, artificial intelligence, machine learning, quantum computing, virtual and augmented reality, autonomous driving, tele-medicine, robotics, big data, the Internet of Things, and blockchain technology, among others. Predicting and quantifying the extent of cyber-risk has become more complex due to the fast-pace adoption of these emerging trends (Pfleeger & Caputo, 2012). What makes digital transformation unique is that it constantly produces new digital assets (Baldini et al., 2020). With the world becoming increasingly digitized, these technological advancements have also over proportionately expanded the attack surface (Brar & Kumar, 2018).

In essence, digital technology is a double-edged sword. While digitalization is primarily associated with efficiency gains, higher productivity, and more convenience, it often exposes users to greater cyber-risks, and enable cybercriminals to exploit new technology (Cook et al., 2023). According to a recent study, a majority of CEO respondents (52%) identified the accelerated pace of technological innovation as the foremost risk factor for cyber-attacks (Dal Cin et al., 2023). Despite this acknowledgement, decisions are often made too hastily whereby security aspects are pushed to the backburner, which can turn into a costly boomerang. Approximately 58% of CISOs indicate that their organizations occasionally adopt new technologies without adequate timeframes for conducting appropriate cyber-security assessments (EY, 2021). This discrepancy could be attributed to cognitive biases such as *overcommitment, bandwagon effect, optimism* or *overconfidence*, or a combination thereof.

Against this background, organizations need to strike a delicate equilibrium between the advantages offered by digital technologies and the potential vulnerability to cyber-threats that accompanies their adoption (WEF, 2023a). A plethora of digital technologies has emerged with the potential to significantly alter the world and the way people work. Examining each of them individually would exceed the scope of this paper. Therefore, the following section will discuss four of these emerging trends and some of their security aspects that need to be considered as examples.

5.3.1 Remote and Hybrid Working Environments

Homes are becoming increasingly more computerized and digital with people often sharing routers and wireless internet access (White, 2015). In fact, 41% of adults have shared their personal account passwords with friends or family members, and 54% access public Wi-Fi hotspots (Olmstead & Smith, 2017a). Especially the COVID-19 pandemic has boosted technology adoption and manifested remote working and hybrid working arrangements (Hancock, 2022; Triplett, 2022). Although employees are being urged to return to the office, more than 40% continue to choose remote work either full-time or for a few days each week. This is equally causing headache for 39% of IT leaders (Cisco, 2023). The rationale behind this concern lies in the fact that remote working has made employees more susceptible to hacking, who are connecting to the corporate network through various access points and different devices. The nature of a home environment tends to be less secure compared to traditional office spaces, making it an attractive avenue for cybercriminals to exploit these weaknesses (Duong et al., 2022; Wash & Rader, 2015). Consequently, this situation has given rise to a variety of additional cyber-threats (Saleous et al., 2023; WEF, 2020), as employees often switch between personal and company devices and communicate through channels outside the corporate perimeter (ACSC, 2022). Ransomware is just one such vicious example of a cyber-threat that can infiltrate the electronic devices of individuals working remotely from their homes without the owner initially noticing it. However, when something goes wrong in remote work environments, research has found that cyber-security incidents are more complex, time-consuming, and costly to resolve. Specifically, security breaches involving remote work were found to correlate with nearly US$1 million, on average, in additional costs, driving up the total costs to an average of US$4.99 million, compared to US$4.02 million per incident outside of remote work environments (IBM/Ponemon Institute, 2022).

Likewise, organizations increasingly embrace the idea of Bring Your Own Device (BYOD), which refers to the integration of personally owned mobile devices such as laptops, tablets, smartphones, or other internet-facing electronic gadgets into the corporate networks of organizations. Users not only access network services provided by the company or institution but also process or store corporate data including confidential PII data of the company's clients as well as other privileged information and files. The conventional demarcation lines between personal and business use are blurring. Meanwhile, work has progressed to a point where it is no longer confined by the boundaries of time, location, or device constraints. Since mobile devices typically have fewer cyber-security controls and protections, they are more frequently targeted by attacks. As such, the risk of falling prey to cyber-attacks has increased due to the ability of employees to use their personal mobile devices to access sensitive corporate data or communicate work-related e-mails outside of office hours (Singh & Bakar, 2019). Accessing a network from a device infected with a virus or trojan poses a threat to sensitive corporate data. Diverse risks are present in today's digital landscape. One such peril is the presence of malicious applications that may come with backdoors and hold the ability to manipulate the user's mobile device. Another crucial factor to ponder is the potential variation in user behavior between personal devices and corporate devices. In general, online behavior often diverges from offline behavior as individuals conform to distinct social norms (Nguyen et al., 2012). In the case of personally owned devices, individuals may be tempted to behave differently in their spare time due to the expectation of heightened privacy. They may be more inclined to share or download questionable content that would otherwise constitute a compliance violation in the work environment, trusting that their own device is inaccessible to the company's IT administrators. Studies have revealed that engagement with online pornography, utilization of various discussion forums, dating platforms, and gaming sites, as well as expenditure on gaming, dating, and pornography sites, were associated with increased victimization (Gainsbury et al., 2019). These findings indicate that specific activities are positively correlated with forms of harm. Furthermore, a survey found that 28% of smartphone owners do not use any screen lock or security features, leaving their personal information vulnerable (Olmstead & Smith, 2017a). When such a device is lost, stolen, manipulated, or compromised, this can cause detrimental consequences. In addition to the potential embarrassment caused by the contents found on the device, any unauthorized surveillance, access, or exposure of confidential corporate information gives rise to liability concerns and expensive legal conflicts that go beyond the individual user and endanger the entire organization.

5.3.2 Application Programming Interfaces (APIs)

Because of today's interconnectedness, it is not necessarily only the actual software or hardware that is vulnerable. Pretty much all applications and databases come with Application Programming Interfaces (APIs) which allow seamless interaction and communication across the IT landscape. APIs serves as the “man in the middle” to share content, protocols, and data between different systems. Software developers heavily rely on APIs to build applications and exchange information. APIs may be used internally or shared with the public. Meanwhile, API calls account for 83% of web traffic, with the majority of such traffic being attributed to custom applications (Akamai, 2019). The mushrooming of applications is a direct outcome of digital transformations and the skyrocketing adoption of cloud computing.

Today, organizations often rely on thousands of APIs with each representing a possible vulnerability. In fact, a recent study suggests that the typical organization uses 15,564 APIs, while large enterprises with a workforce exceeding 10,000 employees, face a significantly higher level of risk exposure, with an average deployment of 25,592 APIs (451 Research, 2022). Because they are so widespread, a real issue arises when an API is being forgotten. An endpoint that has been rendered obsolete, abandoned, or overlooked is then referred to as a “Zombie API”. Such APIs have lost their relevance and usefulness, but still linger in the dark indefinitely, which poses a major security risk. In the same study mentioned before, 41% of participants reported an API related cyber-security incident over the past 12 months. Of those affected, a majority, specifically 63%, reported that the incident resulted in a data breach or loss of data, according to 451 Research. The results indicate that the measures taken are ineffective. Nine out of 10 respondents (90%) reported that their respective organizations have implemented API authentication policies. However, nearly one-third (31%) expressed uncertainty regarding the efficacy of these policies in ensuring sufficient levels of authentication (ibid.).

In 2022, cybercriminals initiated the sale of user data in hacker forums belonging to a substantial number of over 5.4 million “X” users, commonly known as the social media platform Twitter. This was preceded by the exploitation of a compromised API (Keary, 2022). Around the same time, Australia’s second largest telecommunication provider, Optus, disclosed a huge data breach. Through a compromised API, sensitive PII data from 11.2 million customers were leaked comprising names, dates of birth, phone numbers, e-mail addresses, home addresses, and passport and more than 3.6 million driving licenses numbers. The attacker posted two samples each with 100 data records and demanded a ransom of US$1 million in cryptocurrency (Lu & Kurmelovs, 2022). One year later, Optus suffered a nationwide network outage, disconnecting hospital phone lines and payment systems. Over 10 million Australians were without mobile and internet services for 14 hours. This was the second consecutive severe disruption and last nail on the coffin, leading to the CEO’s departure (BBC, 2023).

These are just two examples, but there have been many more. Further, these two examples not only illustrate the magnitude of the scope of vulnerabilities and the severity of the threat, but it also shows that nobody is immune. Even technology companies which should have the skills how to put proper safeguards in place can become victims of cybercrime.

5.3.3 The Internet of Things (IoT)

The Internet of Things (IoT) is experiencing rapid growth, resulting in a significant rise in the number of vulnerabilities that organizations must protect against malicious actors. In a broader context, the 4th industrial revolution (Industry 4.0) refers to the move toward smart factories, enabled through digitalization and automation across industrial sectors. This, among other things, is underpinned by the convergence between Operating Technology (OT) and Information Communication Technology (ICT) as well as the augmentation of industrial processes with smar5t sensors (this is also referred to as the Industrial Internet of Things or IIoT in short) and the commercialization of data. As a result, the proliferation of digital technologies as part of Industry 4.0 has enabled the supply chain to be managed more efficiently.

Besides the opportunity that lies in these digital value chains, they inherently expose firms to additional risks. Following Culot et al. (2019),*"the Internet of Things is exponentially increasing the number of entry points for organizations to defend from nefarious actors. [...] The potential damage of cyber-attacks is substantial in terms of continuity of business operations, theft of confidential information, and reputational harm."* For example, one such eye-opening incident illustrating the downside took place in 2017, when a hacker remotely accessed an internet-connected fish tank of a casino in the United States, that had connected sensors to regulate the temperature, food, and cleaning of the tank, to infiltrate the corporate network and eventually stole and offloaded 10 gigabytes of not further disclosed data to servers in Finland (Schiffer, 2017). Although this is just one example, it showcases how easy it can be for intruders to use these IP connected devices, such as a fish tank, as gateways to access the wider corporate network if they are insufficiently secured.

The dual sidedness of the IoT becomes further evident when realizing that the malware targeting IoT devices doubled within the first half-year of 2022 only, with the total number of cyber-attacks detected within these six months surpassing the cumulative count of attacks witnessed over the preceding four years (ENISA, 2022a). One can only imagine the magnitude of the challenge when considering, as per market projections, that there will literally be billions of these IoT devices out there, with each representing a possible vulnerability (see Chapter 1.2). As much as the IoT provides an opportunity, many of these IoT devices are poorly secured. Threat actors capitalize on that, for example, by using these devices as entry gateways to infiltrate an organization or by hijacking and remotely controlling them to form botnets and unleash DDoS attacks (see Chapter 4.4.3). The abusive scenarios are manifold. Given the skyrocketing number of IoT devices, it is imperative to prioritize and invest in robust security practices to protect against cyber-threats and ensure the trustworthiness of IoT ecosystems.

5.3.4 Cloud Computing

The adoption of cloud computing services is skyrocketing. The COVID-19 pandemic has expedited the expansion of cloud-based services to facilitate the operational procedures. According to analyst estimates, the total global spending on cloud services is expected to reach US$1.3 trillion by 2025 (IDC, 2021).[49] On the flip side of this mega trend, cyber-risk is proliferating too. The huge adoption of cloud technologies provides ample opportunities for cybercriminals to strike. Since cybercriminals opportunistically follow trends in technology, it comes as no surprise that Cloud Service Providers (CSPs) and Managed Service Providers (MSPs) are seen as prime targets (ENISA, 2022a, p. 31). According to law enforcement reports, these providers have increasingly been targeted by ransomware groups as well as state-sponsored actors because of their entrusted network connectivity and privileged access to a myriad of customers (CISA, 2022a). Application Programming Interfaces (APIs) are handy and efficient when it comes to sharing information across applications and microservices. Nevertheless, they also represent another potential entry point for attackers (see Chapter 0). Threat actors exploit any misconfiguration in the company's cloud-hosted internet-facing application and steal user data to sell on the black market (PwC, 2023, p. 31). In addition to facing substantial risks through supply chain attacks, account hijacking is one of the most prevalent and exploitable vulnerabilities, enabling malicious actors to pilfer users' account credentials (Shahid & Khan, 2022).

The threat is omnipresent and there is no slowdown in sight. In May 2022, the cyber-security authorities of the United Kingdom, Australia, Canada, New Zealand, and the United States released an alert informing organizations about the cyber-threats to MSPs and their customers (CISA, 2022b). SolarWinds serves as an eye-opening example. Little had been known about the US-based technology vendor that provides management and monitoring

[49] Cloud computing allows firms to replace or augment local IT capabilities with those of a Cloud Service Provider (CSP) or Managed Service Provider (MSP). The services are typically being rendered in *[X]-as-a-service* model, whereby the assets are owned by the provider and rented by the customer. For clarification purposes, CSPs are specifically responsible for providing cloud services for their customer, whereas MSPs are responsible for potentially managing all the technology needs of an organization including but not limited to cloud services.

software until it became a target of the Russian intelligence agency. However, everything turned upside down in 2020, after a Russian APT group was able to break into the software code, managing to extract confidential data for an astonishing duration of eight months before finally being detected. The attack had far-reaching consequences, impacting 18,000 customers who had downloaded the compromised software (Cordey, 2023). By February 2021, the Russian APT group had already infiltrated at least nine U.S. federal agencies and around 100 private companies, including the Department of the Treasury and the Department of Justice. The United States government networks and critical infrastructure have been compromised by Russian actors through the SolarWinds cyber-attack, which is being considered as one of the most consequential attacks ever launched against the United States (Willett, 2023).

According to research conducted by accounting firm PricewaterhouseCoopers (PwC), spanning 3,522 senior executives across more than 60 countries worldwide, 38% of respondents expect more serious attacks via the cloud (PwC, 2023, p. 31). Another study involving over 2,500 IT leaders revealed even higher numbers, with more than half (51%) of the respondents identifying cloud security as a big concern (Cisco, 2023). The demand need is exacerbated by the ongoing trend of organizations embracing cloud platforms. Such worries are well-founded because a successful cyber-attack hitting a cloud environment can become very costly and is no longer a rare occasion. One of the largest data breaches in history hit Capital One in 2019, the eights largest bank in the United Sates, when a hacker compromised the bank's AWS cloud and illegally obtained confidential PII data of approximately 100 million Americans and 6 million in Canadian citizens (Khan et al., 2022; Novaes Neto et al., 2020). The shares of Capital One plummeted 5.9% upon the disclosure of the incident, resulting in an overall loss of 15% within a span of two weeks (Novaes Neto et al., 2020). Subsequently, a class action lawsuit was filed. Without considering any internal or external costs to restore operations, the company was fined an additional US$80 million by the regulator and agreed a settlement to pay another US$190 million to compensate the affected customers for the privacy violation (Avery, 2022). Meanwhile, according to IBM/Ponemon Institute (2022), 45% of the data breaches reported affect cloud environments. The average costs in hybrid cloud deployments where the lowest with US$3.8 million, compared to US$4.24 million for incidents in private clouds and US$5.02 million for incidents targeting public clouds.[50] The study revealed a 27.6% difference in the

[50] A Private Cloud is a dedicated cloud environment not shared with any other organization. The users of a Private Cloud have exclusive access to it. In contrast, a Public Cloud is a cloud service where multiple customers share the same platform. Hybrid Clouds are a combination of these two approaches.

costs between hybrid cloud breaches and those in public clouds. One explanation for this significant difference may be related to the lack of the user's autonomy and control in public cloud environments which adds complexity in resolving a breach and thus makes it a more costly endeavor. Another study revealed that in comparison to on-premises deployments, organizations are found to exhibit a twofold increase in the likelihood of possessing high-risk exposures when utilizing cloud-based solutions (Cyentia Institute, 2019). However, diversification pays off. Organizations that employ four cloud providers experience a significantly reduced exposure rate, amounting to only 25% of the risk faced by those relying on a single cloud provider. Furthermore, the utilization of eight cloud providers further diminishes this rate by half. Yet such a diversified vendor landscape is still more the exception than the norm with 70% of organizations relying on four providers or less (ibid.).

Moreover, the absence of lucidity in a shared responsibility model may result in the security of cloud services being relegated to a state of ambiguity.[51] As the intricacy of the supply chain and reliance on third-party entities continue to escalate, it is imperative for organizations to attain greater command and transparency over their supplier relationships and dependencies, potentially through the consolidation of their partner network. Despite the remarkable commercial success of cloud computing as such, it is still an area warranting further research in theory and practice as it relates to the application in the supply chains (Ageron et al., 2020).

5.4 Spillover Effects

The intricate nature of digital value chains exposes firms to risks that extend beyond their immediate control. Cyber-attacks can cause devastating spillovers (otherwise known as chain reaction or cascading effects) far beyond an individual firm. However, the term *spillover effect* in the cyber context is not unambiguous and needs further clarification. For instance, Maness and Valeriano (2016) argue that a cyber-spillover is *"when cyber conflicts seep and bleed into traditional arena of militarized and foreign policy conflict"*. Verstraete and Zarsky (2022) refer to cyber-spillover as *"an unrecognized source of positive externalities within*

[51] When it comes to Cloud Computing, the shared responsibility model refers to a security and compliance framework that outlines the responsibilities of cloud service providers (CSPs) and customers for securing every aspect of the environment, according to which the CSP takes care of the security "of" the cloud while customers are responsible for security "in" the cloud. This, for example, implies that physical access to the data center as well as maintenance of the ICT infrastructure is part of the CSP's responsibility, whereas data protection and logical access to the respective system hosted in the cloud is part of the customer's responsibility.

cyber-security". Instead of focusing on negative externalities and market failures, the authors introduce the idea of common users benefiting from heightened cyber-security standards put in place by the Cloud Service Provider (CSP) to protect their entire client base that would have otherwise not been available or affordable individually. Most authors use the term *spillover effects* to contextualize negative cyber-risk (Dieye et al., 2020; Ouellet et al., 2022; Welburn & Strong, 2022), which is vastly different from the two previous examples. What all three definitions have in common though is (i) a trigger event, (ii) that is causing positive or negative consequences, which are, (iii) whether wittingly or unwittingly, (iv) affecting others. With regards to this thesis, emphasis will be put on *negative economic spillovers* resulting from *cyber-security incidents*, translating into *systemic risk*.[52, 53]

While cyber-risk has been introduced before (see Chapter 5.1), systemic cyber risk comes in multiple forms and can be categorized in different ways (Forscey et al., 2022). It is the result of common cause cyber failures and cascading effects (Welburn & Strong, 2022). A cyber-attack can cascade threefold—namely *upstream* (effecting suppliers), *laterally* (effecting business partners) or *downstream* (effecting customers). A related yet different perspective is proposed by Forscey et al. (2022), by grouping downstream and upstream into *vertical failure*, using a different name convention when referring to *horizontal failure* instead of lateral effects and finally suggesting *hybrid failure* when referring to an observed combination of both vertical failure and horizontal failure. Irrespective of name conventions, such cascading effects or failures can unfold across industries and have long ceased to be purely theoretical, as numerous case studies demonstrate.

In 2016, Dyn, a U.S.-based provider of Domain Name Servers (DNS) who plays a crucial role in internet routing, fell victim to a DDoS attack. As a result, numerous online services such as Netflix, Twitter, Spotify, Reddit, CNN, and PayPal were inaccessible for hours across the United States and Europe (Thielman & Johnston, 2016). The attack was performed by an unknown adversary leveraging a Mirai Botnet with more than 100,000 hijacked IoT devices, thereby also illustrating how digital technology can effectively be weaponized to cause havoc (Woolf, 2016). For further botnet information, see Chapter 4.4.3.

[52] For simplification purposes, the terms *spillover* (effect), *domino effect, cascading effect* and *chain reaction* will be treated synonymously.

[53] Though in the context of this thesis, emphasis is put on negative spillovers, it is noteworthy that spillovers are not inherently negative. There can be positive spillovers too. Thus, the word itself is neutral and needs further connotation to indicate a positive or negative nexus.

In 2017, the world witnessed perhaps one of the most wide-ranging cyber-related spillover effects, when NotPetya spread like wildfire within a matter of days. The damages caused by the cyber-attack were devastating for several companies, with Merck suffering losses of over US$870 million, FedEx losing US$400 million, Saint-Gobain facing damages of US$384 million, and Maersk experiencing losses of US$300 million (Greenberg, 2018). Not only were these companies brought to its knees and had operations hampered for weeks, but it also had a significant amplification effect in damages cascading downwards to many of their respective customers (see Chapter 5.5.5 for details).

Due to a human error, a software bug got published across Fastly's network in 2021, one of the largest content delivery networks (CDN) that many other businesses rely upon. Consequently, many internet sites were unavailable including Amazon. Estimates are that this might have translated into a loss of a whooping US$6,803 for literally every second it was down (Hern, 2021). A similar issue occurred the following year in 2022, when Cloudflare—another large content delivery network (CDN) and competitor of Fastly—encountered a routing issue based upon human error. For several hours, hundreds of websites were offline including Amazon Cloud Services (AWS), Google, and Twitter (Swabey, 2022).

These *spillover risks* can no longer be ignored or downplayed considering the facts. It is widely acknowledged that the issue of systemic cyber-risk poses a significant and growing concern, and that these risks are dispersed across various domains of the economy and society, with a multitude of triggers and entry points (Forscey et al., 2022). Meanwhile, a survey conducted by the World Economic Forum (WEF) concluded that 39% of participating organizations had already been affected by a third-party cyber-security incident (WEF, 2023a, p. 18). Such events can serve as a force multiplier and cause significant repercussions. Crosignani et al. (2023) have demonstrated that incidents cascading across the supply chains of the affected firms result in substantial losses for their downstream customers causing damages at least four times greater than those experienced by the directly affected firm itself.

In their study, Scherbina and Schlusche (2023) analyzed a comprehensive dataset comprising publicly reported cyber-security incidents spanning the period from 1999 to 2022. Their research revealed that the announcements of adverse cyber events resulted in negative abnormal returns. The authors further observed that firms with economic linkages experienced a value loss that was equivalent to nearly 45% of the value loss experienced by the directly affected firms. Additionally, the study found that firms with economic linkages smaller than the firm originally hit were impacted more severely than larger firms.

Research by Islam et al. (2022) has found that a cyber-security incident can lead to indirect spillovers—both positive and negative. For example, a non-breached firm in the same vertical may be viewed as a low-hanging fruit and represent an attractive target, potentially having a similar cyber-security posture as the firm previously victimized. Having analyzed a large data set of cyber-security breaches occurred between 2003 and 2013, Wang et al. (2023) have found negative spillover effects among firms in the same industry that offer similar products. On the other hand, a firm in the same vertical as the victim could attract the victim's customer following the breach and thus benefit from the situation. Jeong et al. (2019), drawing upon a dataset comprising 118 instances of cyber-security incidents and 98 announcements of IT security investments spanning the period from 2010 to 2017, suggest that cyber-security incidents provide rival firms an opportunity *"to absorb market power,"* thus constituting a positive spillover effect. According to Islam et al. (2022), empirical evidence implies that spillover effects produce even more uncertainties toward the non-breached firms regarding the repercussions of the cyber-attack on one of their peers. This is consistent with Garg (2019), proposing that detrimental effects of a cyber-security breach are not isolated to the victimized firms. Instead, firms across the same peer group as well as suppliers are quick to follow in taking precautions, thereby already incurring *externalities*.

5.5 Critical Infrastructure

Critical infrastructures are not only the backbone of civilization but also exposed to everyday disruptions encompassing extreme events such as natural hazards, technical failures, and malicious activity including cyber-attacks. The critical infrastructure sectors encompass a range of assets, systems, and networks, both physical and virtual, that are deemed essential. The impairment or destruction of these elements would result in a severe impact on national security, economic prosperity, public health, safety, or a combination of these factors. Various sectors such as financial services, hospitals, ICT services and networks, power grids, and other interconnected networks play a crucial role in upholding essential services. These sectors must operate with utmost reliability, even during times of crisis.

Cyber-attacks on critical infrastructure are troubling yet is has become a prevalent threat (see subsequent subchapters 5.5.1 through 5.5.5). There has been a noticeable surge in cyber-attacks, specifically targeting critical sectors and services encompassing energy, transportation, education, and healthcare (Baldini et al., 2020; ENISA, 2022a). These attacks can be used for espionage purposes, including spying out data; exerting influence, e.g., through disinformation; and sabotage, including disrupting operations. Adversaries are mainly state-sponsored actors, hacktivist collectives, and hypothetically terrorists (see Chapter 4.3.8 for details). The World Economic Forum projects that along with a growing cybercrime, attempts to disrupt critical technology-enabled resources and services will occur more frequently, with attacks anticipated against agriculture and water, financial systems, public security, transport, energy, and domestic, space-based, and undersea communication infrastructure (WEF, 2023b, p. 8). However, the idea of attacking critical infrastructure is not a modern invention. It resembles what military experts refer to as a 'strategic vulnerability', which is defined as follows:

> *"The susceptibility of vital political, economic, geographic, sociological, scientific, or military elements of national power to degradation or destruction by an enemy"* (Dictionary of Military and Associated Terms, 2005).

Already during World War II, the United States and Great Britain sent heavy bombers to drop large amounts of bombs over Germany to cripple the country's infrastructure, demolish its industrial sites and break the population's will to continue fighting (Lewis, 2002).

Going forward, the threat of cyber-attacks against critical infrastructure is realistically only going to grow further as societies around the globe embrace digitalization and increase their reliance on the availability and integrity of digital technologies (think online banking, smart cities, e-government, telematic services, autonomous driving, tele-medicine, and so on). The following subchapters shall provide an overview in excerpts about some of the developments in the respective vertical.

5.5.1 Financial Services

Ever since have financial institutions attracted crime—the digital realm is no different. The emergence of fintech companies and the global trend toward mobile payments have demonstrated that modern banking is a platform-based business that is "asset light". The traditional concept of banking as a physical establishment has become obsolete, as the financial service industry has shifted toward a predominantly digital landscape. Bank robbers have therefore literally exchanged their ski masks, Tommy guns and gloves for hoodies and keyboards. Instead of taking off with squealing tires after a robbery, today's gangsters use more intelligent and astute tactics. The victims often remain completely unaware of their presence until suddenly, their funds mysteriously vanish. Thanks to technological advancements, these heists have become significantly less confrontational and perilous from the standpoint of a criminal. Moreover, these digital innovations have also made these criminal activities outrageously more profitable. As a result, financial institutions continue to be a primary focus of malicious cyber-actors for over a decade (Lewis, 2018, p. 9). Like in the analogue world, banks are exposed in the cybersphere to robbery and thieves too, with the 2016 heist targeting Bangladesh's central bank being one of the most formidable cyber-operations to date, when North Korean *Lazarus Group* succeeded to steal US$81 million from Bangladesh Bank. Despite these enormous amounts, this spectacular operation must be considered a failure as the perpetrators had set their sights on a much larger loot. The attackers successfully submitted 35 SWIFT instructions, instating the transfer of US$1 billion from the bank's account at the Federal Reserve Bank of New York (see Chapters 4.2.1 and 4.3.7) (U.S. Department of Justice, 2018b). Although the first four transfers were executed without hesitation, the fifth one accidentally halted the entire process not due to advanced security measures detecting the scheme, but rather due to fortuitous circumstances arising from a simple typo in the recipient's name spelling (Finkle & Quadir, 2016; Kim, 2022). That way, the North Korean perpetrators only received the first batch of the funds. Otherwise, the full sum would have probably been wired. The magnitude of these raids has never been witnessed in the annals of history, showcasing the vast possibilities that have emerged from the process of digitization, accompanied by its inherent limitations. Even the renowned *Great Train Robbery* in England during 1963 appears tiny in comparison, as it yielded a plunder of £2.3 million, which presently equates to approximately £30 million (British Transport Police, n. d.).

In 2017, there were reports of North Korean hackers trying to infiltrate multiple Polish banks (Chanlett-Avery et al., 2017). Despite their unsuccessful endeavor, it was revealed that the hackers employed remarkably sophisticated techniques, surpassing the expectations of numerous security analysts. Furthermore, researchers discovered a list of additional entities that the North Korean hackers potentially aimed to attack, encompassing prominent financial institutions within the United States and several other nations, including the World Bank (ibid.). Trust is a crucial element for the successful implementation of any novel financial system. Nonetheless, the prevalence of digital heists has become a recurring and troubling theme especially as it relates to cryptocurrencies. Due to the increased anonymity, coupled with limited governmental control and regulation, cryptocurrencies are gaining popularity. Unfortunately, criminals also take advantage of these benefits, making it more difficult for law enforcement agencies to trace money flows. This also applies to abuse cases such as theft, fraud, and heists. In 2022 alone, a staggering amount of over US$3 billion in cryptocurrencies was stolen by malicious cyber actors. The primary targets of these attacks were blockchain bridges, which accounted for 70% of all losses. Additionally, decentralized finance protocols were also targeted, resulting in the siphoning of nearly US$2 billion (Bambysheva & Linares, 2022). Criminals cannot believe in their luck and are rubbing their hands with glee. In the terrestrial world, profits in this order of magnitude are unheard of. However, cyberspace serves as a force multiplier, providing criminals with unprecedented opportunities of abundant illicit gains.

According to the European Central Bank (ECB), half (50%) of institutions reported that they experienced at least one successful cyber-attack during 2021. About 12% were categorized as "significant incidents" (ECB, 2022). Analogously, a total of 79 financial service companies in the United States disclosed occurrences of data breaches in 2022. Notable among these entities were Elephant Insurance Services, a sizable car insurer and a wholly owned subsidiary of UK-based underwriter Admiral Group, and Lakeview Loan Servicing, the fourth-largest mortgage loan servicer in the United States. Each of these incidents resulted in the exposure of PII data belonging to over 2.5 million consumers, encompassing credit and debit card details, as well as other highly sensitive data (Pape, 2022). Apart from creating headlines in the press and eroding trust, such cyber-security incidents can become terribly expensive. According to research outcomes, financial service institutions incurred the second-highest costs per data breach among all industry domains, with an average of US$5.97 million per instance (IBM/Ponemon Institute, 2022). However, as mentioned in previous sections, these figures have the potential to rapidly increase exponentially based on the scale of the incident.

Besides theft, financial institutions are exposed to numerous other cyber-threats including sabotage. In 2018, a remarkable incident occurred when the financial sector in the Netherlands was targeted in a whole series of concerted DDoS attacks. Among the targets were the Dutch tax authorities as well as some of the country's largest banks including ABN Amro, Rabobank, and ING. The online banking services of these major institutions were disrupted for several days. Initially, due to the magnitude of the incident, it was publicly attributed to a state actor and Russia was suspected of being behind the attacks, which triggered a far-reaching police investigation. However, ultimately, an 18-year-old teenager was arrested for carrying out the attacks apparently utilizing a tool that he had purchased for a paltry €50.00 per week from a Dark Web marketplace (Hofmans, 2018). It is hard to comprehend how it was possible for a teenager to take several banks offline using nothing else but pocket money. This case serves as a testament regarding the vulnerability and inefficiency of some of the safeguards implemented. Similarly, New Zealand's stock exchange (NZX) suffered a series of DDoS attacks over four days in a row in 2022, forcing the entire stock exchange to stop trading and the government to activate the country’s National Security System. Although the responsible party for the attack remains unidentified, the incident triggered New Zealand’s central bank to issue a cautionary statement, emphasizing the potential risks cyber-attacks pose to the financial service sector (Hope, 2020). Furthermore, in February 2022, days prior to the Russian invasion of Ukraine, a wave of DDoS attacks occurred in Ukraine taking the websites of numerous banks, government departments, and radio stations offline for several hours (Przetacznik & Tarpova, 2022). This operation was flanked by a disinformation campaign during which Ukrainian citizens received faked SMS messages, claiming that ATM services were down, too. It seems likely, that the attempt aimed at causing fear and panic among the Ukrainian population and possibly triggering a so-called *bank run*, which fortunately did not happen (McLaughlin, 2022). Nonetheless, this was a multifaceted and meticulously executed operation that was later ascribed to the Russian government (Holland & Pearson, 2022).

5.5.2 Utilities

In a 2013 cyber plot, Iranian hackers broke into the command-and-control center of Bowman Avenue Dam in the state of New York, thereby giving them remote access to control the flood gates. While the dam itself is a relatively small one and the attack did not cause damage, this could have been the result of nothing else but sheer luck. Coincidentally, at the time of the assault, the dam’s sluice gate had been manually taken offline for routine maintenance work without the attacker’s knowledge. The event was a huge wakeup call as the infiltration showcased that cybercrime had reached a new level and the prospect of hackers endangering human lives was no longer fiction (Cohen, 2021; Yadron, 2015).

Blackouts are among the most severe threats toward civilization. A wide-spread and prolonged downtime across a region or certain geographical area can have catastrophic effects, potentially affecting a myriad of industry sectors and households. A 2015 study conducted by scholars from the University of Cambridge’s Centre for Risk Studies concluded that a hypothetical severe, yet plausible cyber-attack against a power-grid in the Northeastern United States including New York City and Washington, DC, could leave as many as 93 million people without power, causing—depending on the magnitude and duration of the scenario—anywhere between US$240 billion and US$1 trillion in economic damages (Cambridge Centre for Risk Studies & Lloyd’s of London, 2015). While this may sound apocalyptic, the threat has become real. In December 2015, the world witnessed the first documented power outage caused by a malicious cyber-operation. After three Ukrainian utility providers were hit with malware, hundreds of thousands of homes and businesses and some 225,000 people were left without electricity supply for six hours (Bruijne et al., 2017; CISA, 2021b; Lis & Mendel, 2019; Welburn & Strong, 2022). Further attacks on Ukrainian targets occurred in 2017, which were later attributed to Russian state-sponsored actors (CISA, 2021b; NCSC, 2018). In 2018, the U.S. Department of Homeland Security (DHS) and the FBI jointly published a report detailing a planned cyber intrusion into a U.S. power grid. The report highlighted the risk of state-sponsored actors to exploit this intrusion, thereby causing significant disruption to the power supply and causing wide-ranging turmoil (Welburn & Strong, 2022).

In 2021, a ransomware attack on Colonial Pipeline, the largest pipeline system for refined oil products in the United States, caused a shut down for six days, leading to a widespread fuel shortage and panic buying at gas stations (Crosignani et al., 2023; Forscey et al., 2022). The pipeline is instrumental for fuel supply throughout the Southeast and the Eastern United States, transporting roughly 2.5 million barrels a day (Tsvetanov & Slaria, 2021). The extend of the incident was seen as so severe that it caused U.S. President Joe Biden to declare a state of emergency. An interagency taskforce was immediately summoned comprising resources from the Department of Justice (including the FBI), the Department of Homeland Security (DHS) including the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE), the Department of Defense (DOD), the Department of Transportation (DOT), the Department of the Treasury, the Federal Energy Regulatory Commission, the Environmental Protection Agency (EPA), and the White House Office of Management and Budget (U.S. White House, 2021b). As a repercussion of the cyber-attack, flights at several major airports including Charlotte Douglas International Airport and Atlanta's Hartsfield–Jackson International Airport had to be rescheduled or cancelled in response to fuel shortages (Bair & Blas, 2021). Controversial and equally alarming is the fact that despite significant support from the U.S. government, the incident could not be resolved through technical sophistication or any restoration of the compromised data. The company simply saw no other choice but to fulfill the ransom demands, admitting defeat and ultimately paying approximately US$4.4 million (Alqahtani & Sheldon, 2022). All of this leaves a bitter aftertaste. By meeting the criminals' demands, the very injustice they perpetrate is allowed to prevail. Furthermore, this only serves to embolden these syndicates to continue their criminal pursuit, as they are given the impression that their actions will be met with compliance. Simultaneously, this action sends a highly questionable message to the outside world regarding the state of resilience across critical infrastructure.

Goodell and Corbet (2023) scrutinized the incident from an economic perspective and found *"considerable price reactions and destabilizing volatility"*. Their paper examined the industrial distribution of energy supply in the United States and the cascading effects to the commodity markets following a cyber-attack against an individual firm. Underlining the importance of the topic, Tsvetanov and Slaria (2021) argue that due to comparatively low short-term price elasticity of gasoline demand, supply shocks can exert pressure on household incomes and cut off overall expenditure on other commodities and services, thereby impeding economic prosperity. While the impact on the gas price in this incident varied across locations based on their access to alternative means of fuel supply, shortages and panic buying continued even after the reopening of the pipeline, thereby underscoring the vulnerability of the United States energy sector to potential cyber-attacks.

5.5.3 Healthcare

The healthcare sector is currently undergoing a rapid digital transformation. Emerging technologies offer both efficiency gains and improved patient care. Electronic health records (EHRs), telemedicine, and other advancements have created entirely new possibilities. In the future, the healthcare sector will increasingly adopt and depend on the Internet of Medical Things including interconnected medical devices, big data, smart devices, information systems, cloud services, and other digital technologies (Baldini et al., 2020; Seh et al., 2020). On the flipside of these technological advances, the healthcare sector is increasingly becoming the focus of cybercriminal activities.

Although cyber-attacks targeting the healthcare sector are particularly evil and condemnable since they virtually put human life at risk, this does not stop perpetrators from taking despicable action. The healthcare sector is of interest to criminal groups for different reasons including the sensitive nature of personal health information (PHI). Regardless of the technological advances made, additional reasons lie in the speculation of the perpetrators that some of the legacy systems in the healthcare sector are partially dated, making them easier to infiltrate (Pranggono & Arabo, 2021). For example, in 2014 a series of DDoS attacks was unleashed against Boston Children’s Hospital and several other medical facilities in the area by a hacker who claimed to be associated with hacktivist group *Anonymous*, flooding 65,000 IP addresses with junk traffic to bring business operations to a standstill. The cyber-attack caused a disturbance in the network of the Children’s Hospital for a minimum of two weeks, thereby impeding the availability of internet services utilized by staff to admit and treat patients (U.S. Department of Justice, 2018a). In 2021, the very same hospital got targeted by a state-sponsored actor. The attack was thwarted off by the FBI and attributed to the Iranian government (Milliard, 2021).

In 2017, during the global spread of WannaCry, the United Kingdom's National Health Service (NHS) got hit with ransomware (see Chapter 4.2.1). The cyber-attack resulted in the cancellation of some 20,000 patient appointments with many of them being surgeries (Lis & Mendel, 2019). At the same time, a considerable 26% of healthcare consumers in the United States encountered a breach of their healthcare data. These breaches comprised sensitive information such as their social security number, contact details, electronic medical record, and health insurance identification (Masip-Bruin et al., 2021).

Even during the COVID-19 pandemic, the healthcare sector noticed a significant surge in cyber-attacks (Pranggono & Arabo, 2021). For instance, in 2020, a hospital with one of the largest COVID-19 testing facilities in the Czech Republic got hit with DDoS attacks, forcing a temporary shutdown amid the coronavirus outbreak (Porter, 2020). In the same year, a French hospital near Paris had to cancel operations and transfer some patients after being hit by a cyber-attack and confronted with ransom demands (France24, 2020). Another tragic case happened in 2020 drawing wide-ranging attention, when ransomware disrupted emergency care at a medical facility in Germany, causing a patient to die due to delayed treatment. While the case was initially investigated as a homicide, it was later determined that the patient was in such poor health that the cyber-attack was not solely responsible for her passing (Howell O'Neill, 2020). Besides the rise of attacks in Europe, cyber-attacks in the United States also increased. In 2020, the FBI detected a minimum of 16 instances of ransomware attacks directed towards the networks of healthcare facilities and first responder entities in the United States. These targeted networks encompassed law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, as well as municipalities (FBI, 2021). What all these examples reinforce is that criminals have often neither scruples nor any moral compass.

Despite the end of the COVID-19 pandemic, the threat level in the healthcare sector has not improved. According to Europol, numerous high-profile attacks targeting healthcare institutions, particularly using ransomware, have been reported (Europol, 2022). In 2023, a target list supposedly issued by *Killnet*—a hacktivist group of politically motivated actors in support of the Russian government—leaked, suggesting that healthcare providers across NATO countries including Denmark, Germany, Norway, the Netherlands, the United Kingdom, and the United States are in the crosshairs of DDoS campaigns (Muncaster, 2023; Scroxton, 2023).

The healthcare sector is subject to extensive regulations, making it one of the most tightly regulated industries. As such, the consequences of cyber-security incidents can become correspondingly burdensome. Between 2015 and 2020 only, an alarming number of healthcare breaches occurred, resulting in the exposure of sensitive data that impacted a staggering population of over 157 million individuals (Seh et al., 2020). Over the past 12 years, there has been a significant surge in the costs associated with data breaches in the healthcare sector. Currently, the average cost of a data breach amounts to US$10.1 million. Notably, these costs have seen a substantial increase of 41.6% within a single year (IBM/Ponemon Institute, 2022).

5.5.4 ICT Services

As established before, ICT companies and networks, especially teleconnection companies, Cloud Service Providers (CSPs) and Managed Service Providers (MSPs) are in the crosshairs of threat actors (see Chapter 5.3.4 for further discission). The market for Cloud Computing largely represents an *oligopoly*, that is, that the market is dominated by a small number of suppliers. In fact, 75% of organizations host their assets at the top-5 providers (Cyentia Institute, 2019). The phenomenon of a larger network or community of users being more valuable to each individual member is commonly referred to as *network externality* within the field of economics. With giants such as Amazon Web Services (AWS), Google, and Microsoft each hosting millions of users, a severe cyber-security incident at one of these organizations could have unprecedented economic effects (see Chapter 5.4 for details). To put things into perspective, there are more than 345 million people currently using Microsoft 365 (paid seats) and AWS has the largest customer base of any cloud provider with more than 1.45 million businesses worldwide (Gleason, 2023; Insights, 2022). Google, with its workforce surpassing 88,000 people, is another eye-opening example. This extensive group of employees collectively holds access to the personal information of over 1 billion users globally who interact with Google’s products and services (Kostyuk & Wayne, 2020). The concentration of power underpinned by a tendency toward monopolization within the tech space has already triggered scholars to voice antitrust concerns (Khan, 2017). If one of these tech giants experienced a breach or outage, the potential loss of productivity in the economy due to the unavailability of data, videoconferencing, and cloud services would be immense. A study conducted by Lloyds of London (2018) estimates that an incident that takes out a top-three cloud provider in the United States for 3-6 days would result in financial damages between US$6.9 billion and US$14.7 billion. With increasing cloud adoption projected over the next couple of years, the dependencies will most likely grow even further.

Once again, it is evident that this is no longer a mere theoretical concept. In 2019, a South African internet service provider (ISP) fell victim to a cyber-attack over the course of a weekend, thereby cutting off parts of the country from the internet. The attackers employed a DDoS technique known as “carpet bombing,” which has proven to be highly effective when targeting ISPs, cloud services, and data centers (Cimpanu, 2019).[54] This example clearly illustrates the dilemma. Regardless of a company's robust and sophisticated cyber-security measures, an unavailable internet connection can lead to severe consequences. In other words, the entire operation comes to a grinding halt. Even if a forward-thinking organization has created redundancies and is able to perform a failover to a second ISP, it can still take several hours to propagate a rerouting, resulting in the unavailability of networks, services, and websites in the interim.

In late 2021, there had been a noticeable surge in cyber-attacks by Iranian threat actors against IT services companies with the objective of infiltrating their customers' networks causing the U.S. authorities to issue an official warning bulletin (CISA, 2021c). This trend is significant as it has the potential to exploit more organizations by leveraging trust and access within the supply chain and using these ICT companies as a gateway to target a broad range of victims. By the same token, Microsoft has detected several instances of Iranian threat actors targeting the IT services sector in their efforts to steal downstream customer log-in credentials, thereby facilitating subsequent attacks (Microsoft, 2021).

5.5.5 Transportation and Logistics

In a world of global trade and commerce, transportation and logistics companies are indispensable to fuel the economy. The transportation and logistics sector plays an extremely important key role that probably cannot be matched by any other industry. Logistics serves as the backbone of the economy and concurrently represents a booming economic sector. Countless goods and raw materials are transported daily across the globe. Maritime transportation accounts for 80% of global goods movement, necessitating over 160 million container shipments annually (United Nations, 2022). In 2021, the Parcel Shipping Index observed the transportation of a staggering number of parcels across 13 countries. The daily volume of shipped parcels reached an impressive 436 million, resulting in a remarkable annual total of 159 billion shipments (Pitney Bowes, 2022). The projection for global parcel volume

[54] Unlike a regular DDoS attack that produces a massive data tsunami, carpet bombing reveals a widespread assault in which each individual attack is so small that it bypasses security tools. The firestorm then spreads extensively across the network, causing the infrastructure to collapse. Unfortunately, the attacker can relatively easily repeat the procedure so that even if one wave of attacks has been contained, new waves will be unleashed to cause prolonged downtime.

by 2027 indicates a strong growth trajectory, with estimates ranging from 216 billion to 300 billion annual parcel shipments (ibid).

Many industry sectors rely on *Just-in-Time Delivery* and *Just-in-Time Production*. Following the notion of *Lean Management*, firms utilize these strategies to streamline and reduce the cost of the value creation process, as it significantly cuts the need for inventory storage. However, disruptions in the supply chain leave little room for error. The lack of proper logistics, therefore, possesses the capacity to impede global trade. The transportation and logistics sector remains a fragile ecosystem that is vulnerable to interruptions owing to its vast interdependence and exchange of information, encompassing interconnected container terminals, the monitoring, tracking, and tracing of shipments, package delivery, and automated sorting facilities. A single cyber-security incident in this sector can trigger a supply shock, impacting many industries and costing billions. With Maersk and FedEx being two examples that have been hit hard with ransomware during the spread of NotPetya, the logistic sector is prone to cyber-attacks (see Chapter 4.2.2). While Maersk only experienced a drop of 20% in volume following the ransomware attack (Crosignani et al., 2023), costs quickly accumulated in the back with estimates ranging anywhere from US$200 million (Anderson et al., 2018) to US$300 million (Crosignani et al., 2023; Welburn & Strong, 2022).

What was most likely carried out as a supply chain attack through a compromised website, British Airways experienced a huge data breach in 2018, exposing PII data of roughly 500,000 passengers including log-in credentials, name and address, payment cards, and travel booking details. Despite the public embarrassment caused, the airline can still consider itself lucky. While the responsible regulator, the Information Commissioner’s Office (ICO), initially considered to impose a fine of US$220 million for the GDPR in reflection of the severity of the violation, after two years of investigations, the fine was ultimately reduced to as little as US$26 million (Riley, 2019; Tidy, 2023a). Although there is the saying that lightning never strikes twice, package and mail delivery provider Pitney Bowes was ill-fated and encountered two ransomware attacks in less than seven months. With more than 1.5 million customers around the globe, including 90% of Fortune 500 companies, the attacks encrypted several IT systems and lead to a partial system outage affecting numerous industries (Gatlan, 2019). The company disclosed a US$29 million dent on free cashflow and a US$19 million cut in EBITDA in February 2020 before the second attack hit the organization shortly thereafter in May 2020 (Nolan & Fixler, 2021).

CHAPTER 6
RESEARCH GAPS AND EMPIRICAL FINDINGS

6.1 Identification of Research Gaps

This section aims to identify and discuss the key research gaps in the current literature, highlighting areas where further investigation is needed. The goal is to create a comprehensive understanding of the topics that have already been explored and to identify where additional research could advance the field. The subsequent subsections will delve into these gaps with greater specificity.

6.1.1 Decision-Making in Cyber-Security

The decision-makers in the cyber-security domain are immediate stakeholders who carry a significant weight of responsibility. Their roles are crucial, as their decisions directly impact the security posture of organizations and individuals alike. At the same time, the realm of cyber-security is characterized by its ambiguous and diverse nature, presenting decision-makers with perplexing conditions. Within this dynamic context, it becomes evident that decision-makers are unable to sustain utmost rationality in their decision-making processes (Dong et al., 2021). This challenge is compounded by the rapid pace of technological advancement and the evolving nature of cyber-threats. Thus, their actions are susceptible to cognitive biases too, which may lead to sub-optimal or even hazardous results (Jalali et al., 2019; Kianpour et al., 2021).

With the global economy having moved into a post-pandemic era and an increasing number of activities shifting to online platforms, the stakes in decision-making processes related to cyber-security are higher than ever. The responsibility of making decisions that impact the cyber-risk posture is growing, especially for individuals in the work environment (Bahreini et al., 2023). Indeed, users click on links, access, and download online content, share, and disclose data and information, and so on. This surge in digital activity amplifies the complexity of cyber-security management. It requires IT professionals and cyber-experts to make material decisions on how to conceptualize their organization’s cyber-security architecture, which tools to deploy and not to deploy, how to respond to cyber-threats and alerts, and much more. It also implies a continual underlying battle and delicate trade-off between usability and security. All these choices encompass various strategic decisions that have the potential to yield adverse consequences.

Irrespective of the rapid development of technology, humans remain the principal agents and assume a crucial responsibility in overseeing and endangering the safeguarding of the cyberspace (Bone, 2016; Gunawan et al., 2023; Kovačević et al., 2020). Although previous studies reviewed different angles on cyber-security behavior, research lacks a comprehensive study which scrutinizes the biases in cyber-related decisions specifically across subject matter experts such as IT professionals and cyber-security professionals. Understanding these biases is critical, as it could lead to more informed and effective strategies for managing cyber-risk.

6.1.2 Misconceptions and Psychological Barriers

Both empirical evidence and anecdotal evidence show that there are still plenty of misconceptions. A prevailing one is that if individuals were provided with sufficient information, they would undoubtedly take the appropriate safeguards (Allen et al., 2020). Despite recognizing the significance of cyber-security, numerous leaders within organizations struggle to fully comprehend the magnitude of damage that can be inflicted by cyber-attacks (Rahman et al., 2021). This issue is exacerbated by Spence's Model of Signaling, where organizations often prioritize visible compliance over substantive security improvements.[55] Furthermore, they lack a comprehensive strategy to adequately equip themselves in preparation for and mitigation of these potential threats (Allen et al., 2020). Management often engages in a narrow-minded approach, fixating on meeting regulatory requirements and utilizing metrics to demonstrate their productivity, without fully comprehending the impact of their decisions (Hielscher et al., 2023). Imperfect information also plays a role, as customers are often unable to thoroughly "kick the tires" when it comes to testing cyber-security products. While they might run Proof of Concepts (POCs), these typically only assess the admin consoles or integration aspects and do not account for specific attack scenarios that may be challenging to simulate. As a result, the validity of these POCs remains questionable, leaving organizations to make purchases in blind faith based on *signaling* and *anchoring*, hoping they are not misled. At the same time, the allure of "silver bullet" solutions continues, with many relying on single technologies that promise comprehensive protection but often fall short. Herding behavior and bandwagon effects further compound this issue, as organizations tend to follow industry norms and their peers rather than critically assessing their unique cyber-security needs. This often results in market structures characterized by a "the winner takes it all" dynamic, where certain

[55] Andrew Michael Spence, awarded the Nobel Prize in 2001, is an American-Canadian economist, celebrated for his work on signaling in markets with asymmetric information.

firms emerge as dominant players (Anderson, 2001). Such widespread adoption of a dominant technology can introduce *systemic risk,* as witnessed recently with the CrowdStrike outage, which caused what was labeled a “global IT meltdown”, affecting millions of PCs worldwide (Williams, 2024). Cyber-security incidents, which have inflicted substantial financial losses on renowned companies, led to the resignation of CEOs, negatively affected stock prices, and eroded trust. Nonetheless, a recent survey of 1,000 CEOs revealed that over half believe the cost of implementing cyber-resilience measures exceeds the cost of experiencing a cyber-attack (Dal Cin et al., 2023). Despite the crucial role of digital technology in modern societies, there is still a lack of understanding about the causes, effects, and potential consequences of service outages (Franke, 2020).

6.1.3 Financial Implications

Understanding the financial and operational impacts of cyber-security incidents is essential for grasping the broader implications of poor decision-making within the cyber domain. The significant increase in the frequency of cybercrime, which is becoming ever more widespread and impactful, underscores the growing risks (Brar & Kumar, 2018; Cremer et al., 2022; Huang et al., 2018). As discussed earlier, research highlights that roughly 9 in 10 data breaches can be attributed to human error, emphasizing how detrimental inadequate decision-making can be (Hancock, 2022). This issue is underscored by the increasing prevalence of cybercrime, which poses significant peril to global economies, businesses, and national security (Baldini et al., 2020; Gunawan et al., 2023; Konradt et al., 2016; Sviatun et al., 2021). A wealth of anecdotal and empirical evidence illustrates the enormous financial losses companies have endured following cyber-security incidents (Nikkhah & Grover, 2022; Rundle, 2019; Sharma et al., 2021; Welburn & Strong, 2022). Publicly listed companies see an average stock price drop of 7.5% and a market capitalization loss of over US$5.4 billion following a data breach. For example, Okta’s market capitalization fell by US$6 billion after disclosing a breach involving a third-party supplier, significantly affecting its financial standing (Huang et al., 2023). Similarly, Equifax, a U.S. financial service firm, faced staggering losses exceeding US$700 million following a data breach caused by human error (Lynch, 2017; Prior, 2019). Other sources even put the figure at over US$1 billion for a cyber-security incident that was labeled as “entirely preventable” (Jaeger, 2020). Emphasizing the tragic nature of this incident is that the whole event unfolded due to an error made by a single employee (Lahcen et al., 2018). While this might be seen as an extreme scenario, large-scale cyber-security incidents are no longer a rare occurrence. In 2013, Yahoo suffered a US$350 million loss from a massive data breach, which exposed PII data for 3 billion accounts and was the largest incident at the time (Mullen & Fiegerman, 2017). However, this was only the beginning and many other sizable incidents have followed, affecting Amazon (US$877 million), Morgan Stanley (US$120 million), T-Mobile (US$350 million), Uber (US$148 million), and several others (Sharma & Hill, 2023). Nevertheless, it is crucial to acknowledge that these numbers depict a fraction of the total consequences, as there have been countless other incidents that have either remained undisclosed or escaped attention. When it comes to large scale cyber-security breaches exposing millions of confidential data sets, the average costs for such an incident have meanwhile climbed to a remarkable US$387 million (IBM/Ponemon Institute, 2022). Based on empirical evidence, there was a notable escalation in the quantity of compromised data records, which grew nearly threefold from 4.3 billion in 2018 to a shattering 11.5 billion in the year 2019 alone (Novaes Neto et al., 2020).

Cybercrime has become the primary reason for data center outages, indicating the escalating risk posed by malicious actions in the digital realm (Ponemon Institute, 2016). Moreover, the financial ramifications of these incidents are eye-opening as the average expense of an unplanned outage was around US$9,000 per minute and approximately US$540,000 per hour. The impact of interruptions on firms can vary significantly, where a minor disruption may have minimal implications, but a major outage could pose a threat to the financial stability of the company (Vecchio, 2016). Particularly in certain industries and larger enterprises, the financial repercussions can quickly climb to millions of U.S. dollars per hour (Wang & Franke, 2020). For instance, a five-hour network outage at Delta Airlines resulted in a financial loss of US$150 million (Isidore, 2016). Peak Hosting, an American data center provider, experienced a major setback when it encountered a two-hour outage. This unfortunate incident led to the departure of their largest clients, forcing the company to file for bankruptcy (Stech, 2016).

There is also statistical evidence that cyber-security breaches become more expensive (Algarni & Malaiya, 2016; Kovačević et al., 2020; Nikkhah & Grover, 2022) with the average costs of such an incident having grown by 12.7% compared to the previous year (IBM/Ponemon Institute, 2022). Especially revenue-based regulatory fines (such as those imposed by the European Union’s General Data Protection Regulation or GDPR in short) and class-action lawsuits following a data breach, can turn any misfortune in cyberspace into a very costly undertaking and open Pandora’s box. At the same time, the probability of encountering such an incident has grown significantly over the past five years (Frank, 2020). In the coming years, it is expected that the financial consequences associated with breaches of data privacy will rise substantially, driven by heightened regulatory oversight that accompanies the growing integration of digital technologies. Projections suggest that by 2025, privacy laws will extend their coverage to encompass around 75% of the world's population, signifying a substantial broadening of their reach compared to a mere 10% in 2020 (Gartner, 2020, 2023). Some 142 countries have either implemented or are currently working towards enacting comprehensive data privacy laws, often inspired by the GDPR (Chander et al., 2020). In an increasingly borderless digital society, attempts to control where data resides may seem counterintuitive. However, such control is either explicitly required or indirectly enforced by many new privacy laws (Gartner, 2023). As such, in the event of an infringement, the number of potential claimants could grow significantly, potentially leading to exponentially higher damages.

6.1.4 Counterfactual Thinking and Measurement Error

Research indicates that there is a widespread misconception about one's vulnerability to cyber-attacks, along with an unjustified belief in one's own level of security (Ament, 2017; Ament & Jaeger, 2017). Despite organizations dedicating substantial investments in training their employees on cyber-security measures, a significant portion of their workforce tends to exhibit overconfidence in their ability to effectively combat cyber-security breaches and incidents (Frank, 2020; Rhee et al., 2012). The common perception of the internet frequently centers on its image as a reliable platform for exchanging information, carrying out transactions, and exercising authority over tangible objects. The considerable trust bestowed upon the internet's safety plays a crucial role in fostering a sense of reduced vulnerability to cybercrime and the erroneous notion that cyber-threats are not of grave concern (De Kimpe et al., 2022). Even though most individuals view the internet as a secure space and utilize it regularly through their smartphones, tablets, and computers, there is a significant volume of daily cyber-attacks (de Bruijn & Janssen, 2017). The ambiguity regarding the dramatic underestimation of costs and probability of occurrence are just one illustration of how cognitive flaws and shortcuts cause dysfunctional outcomes. The media also shapes public awareness and understanding of risk. Factors like amount of coverage, framing, tone, credibility, format, and channels all influence how people perceive negative events (Paek & Hove, 2017). However, the media has extensively covered cyber-security incidents, which have effectively heightened public attention regarding the detrimental consequences of cyber-threats (Hooper & McKissack, 2016; Loonam et al., 2022). Consequently, the absence of media coverage or infrequent reporting can hardly serve as a plausible justification for a deficiency in cyber-risk awareness, thereby increasing the likelihood of judgmental errors. People often focus on parts of a message that support their beliefs, ignoring anything that challenges them. This occurrence is commonly referred to as the existence of a *confirmation bias*. Such a selective hearing hampers effective communication and understanding of complex issues (de Bruijn & Janssen, 2017). Especially *optimistic bias* or *unrealistic optimism* leads individuals to believe that risks pose a lesser threat to themselves compared to others (Weinstein, 1980). A striking finding suggests that senior executives often exhibit a greater level of overconfidence than the average person (Dong et al., 2021). In general, such *heuristics* and cognitive *biases* lead to suboptimal decision-making with wide-ranging economic repercussions. These observations are consistent with findings from other studies, suggesting that even emergency responders in high-stake situations, including disaster response and medical emergencies, are prone to misjudgment, too (Brooks et al., 2020; Simpson & Lyndon, 2019). Similarly in the cyber domain, due to the increasing interconnectivity of value chains and interdependencies, there is more at stake. Cyber-risks can quickly arise that extend far beyond an individual company and turn into *systemic risk* (Schwarcz, 2008; Welburn & Strong, 2022). In the blink of an eye, poor decisions can cascade onto unrelated third parties, who are suddenly affected by system failures, supply shortages, and data breaches, causing harm to their operations (Forscey et al., 2022). This has already been revealed by numerous instances including ransomware campaigns such as WannaCry or NotPetya (see Chapters 4.2.1 and 4.2.2 respectively), a cyber-attack on a powerplant causing a blackout affecting several hundred thousand households (see Chapter 5.5.2), and a variety of large-scale internet outages (see Chapter 5.4). And when push comes to shove, the performance of cyber-security incident response is again hindered by the presence of judgmental errors (Lemay & Leblanc, 2018). All these interrelations and dependencies ultimately contribute to an exponentially growing cyber-risk posture.

The evident misunderstanding of CEOs in this context can be elucidated by the dearth of counterfactual thinking. Consequently, the absence of identified cyber-security incidents may reinforce an individual’s conviction in the security posture of their organization, leading them to erroneously perceive correlation as causation (Ting, 2019). Another issue in the domain of cyber-security pertains to the existence of significant psychological barriers, as there is no easily identifiable capital return, unlike other expenditures. Given that cyber-security decisions involve intricate tradeoffs, including the advantages and disadvantages linked to revealing or safeguarding sensitive assets, it appears logical to apply a rational decision-making model (Acquisti et al., 2017). As a result, questions regarding the effectiveness and necessity of these measures quickly come to the forefront (Fielder et al., 2018). Put simply, organizations want a business justification and see that their investment “pays off” (Ward et al., 2008), which may be difficult to proof in case of technology investments which are primarily geared toward prevention of adverse events. For a non-tech company that is not inherently digital but undergoing a transition towards the digital realm, understanding the significance of digital assets can be unfamiliar territory for decision-makers. Furthermore, the inherent invisibility of digital assets, specifically data, poses a potential risk as individuals may not prioritize the protection of these assets to the same extent as they would for tangible assets. The discrepancy between the measured quantity and its accurate value is known as *Measurement Error* or *Observational Error*. Underinvestment can be a sequel of these judgmental errors (Garg & Camp, 2011; Ting, 2019). It is therefore not surprising that within the cyber domain, the proverb *"there is no glory in prevention"* circulates. This vividly underscores the dilemma.

6.1.5 Cyber-Risk Exposure

One of the most significant obstacle in comprehending cybercrime pertains to the vast and complex nature of its landscape (Arief et al., 2015; Dal Cin et al., 2023). As such, cyber-threats have emerged as a significant concern for organizations across numerous verticals (Cossin & Lu, 2021; Dal Cin et al., 2023; EY, 2021), particularly those heavily dependent on digital technologies (Buckland et al., 2015; Huang & Madnick, 2017; WEF, 2023a). Regrettably, the level of awareness regarding the magnitude of the issue has made minimal progress over the course of time (Armin et al., 2015). Many organizations continue to exhibit inadequate performance in managing cyber-risks (Jalali et al., 2019).

While building cyber-resilience should be seen as a highly strategic question for the boardroom, apparently that is often not the case. Surprisingly, a mere 15% of CEO respondents arrange dedicated meetings on cyber-security (Dal Cin et al., 2023). The CEO and the company's board might not be prioritizing the matter appropriately because of the presence of *heuristics* and *biases*, presenting a possible reason for their lack of attention. The fact of the matter is that insufficient awareness and comprehension of cyber-threats can lead individuals to undervalue the potential consequences they may face, both personally and financially. Moreover, biases in risk evaluation contribute to underestimating the likelihood of experiencing a cyber-security incident that poses a direct threat to their personal information (Kostyuk & Wayne, 2020). Only 33% of CEOs strongly agree that they have deep knowledge of the evolving cyber-threat landscape and the potential cost their organization could incur from cyber-threats (Maynard et al., 2018). Making matters worse, CISOs find their advice is being disregarded. Nearly half (43%) report that they have never felt more worried to handle the ever-growing cyber-threat (EY, 2021). In parallel, a significant number of enterprises are contending with the issue of employee burnout alongside a dearth of cyber-security staff (Triplett, 2022).

CISOs often find themselves overwhelmed and exhausted due to the constant demands of their role, leading to a sense of being undervalued and misunderstood (Hielscher et al., 2023). The immense workload and responsibilities placed upon them can take a toll on their well-being and overall job satisfaction. These observations align with the findings of Heidrick & Struggles, who found that CISO participants in the United States identified stress (60%) and burnout (53%) as their main personal risks. Likewise, in Europe, CISO respondents reported stress (54%) and burnout (35%) as the primary concerns (Aiello et al., 2022). Perhaps most striking is that amidst the already tense situation, a significant 41% of participants indicated that their organization lacks a succession plan for the CISO position (ibid.). This lack of preparedness may result in a significant vacuum and heightened vulnerability in the event of the role becoming vacant.

To effectively gain cyber-resilience, it is therefore imperative to overcome the barriers outlined, understand the driving forces behind the cybercrime ecosystem, and type of actors and the motives of the adversaries who are counting on human error and flaws in human decision making. Due to the growing prevalence of digital technology, the situation is further exacerbating. Organizations inevitably keep broadening the attack surface (Brar & Kumar, 2018; IBM/Ponemon Institute, 2022; Jalali et al., 2019; Vagle, 2020a). Thus, it is imperative for organizations to comprehend the cyber-risks and vulnerabilities associated with these technologies, as well as the consequences of exploitation. This understanding is crucial and a lot more cost effective for enhancing the awareness of professionals in the field and offering them guidance on mitigating cyber-risks (Bernik, 2016).

6.1.6 Organizational Barriers

Establishing a culture of cyber-security cascades from the top of the organization and is contingent upon the leadership's commitment to it (Rothrock et al., 2018). The perception of CISOs as merely middle managers infers that cyber-security might be downplayed, treated as a procedural necessity rather than a strategic priority. The board's role in setting the right tone is crucial, and senior management must lead by example to reinforce the message (Cossin & Lu, 2021). Despite the obvious need, there is a long way to go. While the importance of leaders in cyber-security is undeniable, there is a gap in the literature on their role as human factors in organizational cyber-security (Triplett, 2022). A pivotal aspect of the oversight procedure involves the exchange of information and submission of reports between the board and the CISO. The CISO is responsible for providing updates to either the CEO, the board itself, or a specifically assigned committee, regarding the status of cyber-security and guaranteeing sufficient readiness to avert breaches. It is therefore imperative for the board of directors to ensure direct interaction with the CISO (Cossin & Lu, 2021; Loonam et al., 2022). This, in turn, enables the board to fulfill its fiduciary obligation to properly supervise the organization. However, that is easier said than done with approximately one-third of cyber leaders still identifying the acquisition of leadership support as the most difficult aspect (WEF, 2023a). Other studies have yielded comparable results. For example, across 30 separate interviews, CISOs expressed concerns about their dysfunctional relationship with boards, suggesting top-level buy-in may not be as prevalent as believed (Hielscher et al., 2023). If CISOs are not empowered and are viewed merely as technical experts rather than strategic leaders, it reinforces the misinterpretation of cyber-security as an IT issue, rather than a broader organizational concern. In essence, the CISO function can be described as a senior-level executive role rather than that of a specialized technical expert (Shayo & Lin, 2019). To work on eye-height across the C-Suite, CISOs must also gain business acumen and the ability to foster strong interpersonal relationships and cultivate strong bonds (Triplett, 2022). However, this perspective has not yet been fully established or solidified. The role is currently undergoing a transitional phase, only slowly gaining prominence, and being elevated to the executive level. Despite ongoing *digitization* efforts, cyber-security often remains a secondary concern rather than a core strategic priority. For example, in a study comprising more than 1,300 participants, 70% of respondents still identified the IT department as the primary entity responsible for managing and making decisions regarding cyber-risk (Marsh/Microsoft, 2018). Typically, the reporting structures of the CISO will differ based on various elements, including the industry, mission, maturity, resources, capabilities, culture, risk exposure within an organization, and so on (Shayo & Lin, 2019). However, direct reporting is a fundamental element in establishing a well-structured and methodical approach to effectively address cyber-security concerns (Loonam et al., 2022). According to research conducted by Kwon et al. (2013), organizations that have CISOs holding a seat on the board and possessing the ability to effectively communicate with other board members have negatively correlated with the likelihood of experiencing cyber-security incidents. Nonetheless, despite the C-Suite designation, many CISOs still find themselves operating as middle managers, reporting to other functional areas like the Chief Information Officer (CIO), Risk Management or Compliance (Lowry et al., 2022). In fact, a study undertaken by executive search firm Heidrick & Struggles reveals, only 14% of CISOs are part of corporate boards or advisory boards (Aiello et al., 2022). This lack of empowerment and visibility further limits their ability to influence decision-making at the highest levels, which may contribute to a false sense of security within the organization. Many

CISOs acknowledge their limited authority (Hielscher et al., 2023). The observed absence of empowerment ultimately acts as a barrier, thereby limiting the effectiveness of CISOs. If they are perceived as mere middle managers, they may find themselves handcuffed in their ability to support the company's overall objectives and goals (Maynard et al., 2018). Moreover, with the increasing demands for compliance with escalating privacy requirements referenced earlier, CISOs face an additional burden. In many organizations lacking a specialized privacy function, responsibility for these requirements is often passed onto technology, particularly the cyber-security team under the CISO (Gartner, 2023). This dual responsibility not only heightens stress and the risk of burnout but also leaves the organization more vulnerable to cognitive biases and errors in both cyber-security and privacy compliance.

6.1.7 Summary

In recent years, scholars have begun directing their attention towards the examination of misperceptions within the realm of cyber-security defense, as well as delving into the field of decision-making research (e.g., Bone, 2016, 2021; Garg & Camp, 2011; Jalali et al., 2019; Lemay & Leblanc, 2018) and human cyber-security behavior (e.g., Alsharida et al., 2023; Hadlington, 2017; Hong et al., 2023; Krawczyk et al., 2013; Safa et al., 2015; Waldrop, 2016). Some cyber-related studies have specifically dealt with *optimism bias* (e.g., Alnifie & Kim, 2023; Eling & Jung, 2024; Fatoki et al., 2024; Hewitt & White, 2022; Rhee et al., 2012), *anchoring* and the *illusion of control* (e.g., Ceric & Holland, 2019; Mancuso et al., 2013), *overconfidence* (Ament, 2017; Ament & Jaeger, 2017; Dong et al., 2021; Frank, 2020; Gibbs et al., 2017; Rhee et al., 2012), *loss aversion* (Pratama & Firmansyah, 2021), *prospect theory* (Qu et al., 2019), *framing* (e.g., de Bruijn & Janssen, 2017; Gomez & Villar, 2018; Rosoff et al., 2013), and *nudging* (e.g., Acquisti et al., 2017; Hartwig & Reuter, 2021; Zimmermann & Renaud, 2021). Others have looked into adverse consequences such as risk exposure (Fielder et al., 2018), moral hazard (Vagle, 2020a), or underinvestment (e.g., Gordon et al., 2015; Ting, 2019). Despite the prevailing emphasis on cyber-security, there exists a lack of research that is connecting the dots and concentrates on the behavior-related dimensions within this realm, particularly the mitigation of risks by subject matter experts. This gap in knowledge underscores the imperative for further analysis to foster a deeper understanding of these pivotal issues.

Scholars have drawn upon theories from multiple academic fields, including sociology, psychology, and criminology, to discern the determinants of individuals' intended and actual behaviors. Consequently, a thorough analysis of the available literature was conducted to identify the models and theories relevant to cyber-security awareness and behavior. This examination encompassed diverse contexts, including adherence to information security policies, to provide a comprehensive understanding of the subject matter.

In 2012, a seminal study by Rhee et al. was published in *Computers & Security* (Impact Factor: 4.8, h-Index: 125), which is considered be one of the most respected journals in the cyber-security domain. Their research explored the impact of *optimism bias* and the *illusion of control bias* on risk perception within the cyber-security realm, focusing on so-called Management Information System (MIS) executives in the United States. This pioneering research provided critical insights into how cognitive biases affect risk assessment and decision-making in cyber-security. The paper has garnered more than 100 citations. Nonetheless, the cyber-security landscape has undergone significant changes over the past decade, marked by a substantial increase in cybercrime, heightened awareness and understanding of cyber-threats among professionals, and a much larger attack surface underpinned by the skyrocketing adoption of emerging technologies. Consequently, it is essential to reassess and broaden the initial study to ascertain the impact of these changes on experts' risk perceptions.

This thesis expands on Rhee et al.'s (2012) original research by incorporating additional cognitive biases, such as *overconfidence* and the *availability heuristic*, into the examination of cyber-security risk perceptions. It also broadens the geographical scope to include experts from Germany, Austria, and Switzerland. This research aims to provide further insights into the evolving landscape of cognitive biases in cyber-security risk perception and contribute to the development of more effective risk management strategies.

6.2 Assumptions of the Empirical Study

Geographical Scope: To the best of the author's knowledge, the examination of cyber-related biases has not yet been conducted across Germany, Austria, and Switzerland, with an emphasis on subject matter experts, creating a gap in the current research. By broadening the geographical scope beyond the United States, where the original study took place, this research contributes to filling this void and offers valuable insights into potential cultural variations in cyber-security perceptions and biases.

Shifting Focus: The previous research focused on MIS executives, potentially skewing results towards general IT management perspectives. In contrast, the present study emphasizes engaging cyber-security experts, resulting in a more nuanced understanding of cyber-security issues. In the present research, only a third of participants identified their job function as Information Technology, reflecting a more informed demographic. This shift ensures a comprehensive view informed by professionals specializing in the cyber domain, addressing biases and providing relevant insights for today's challenges in the field.

Temporal Changes: The original study took place more than a decade ago, and since then, the cyber-threat landscape has undergone significant changes. This dissertation seeks to provide an up-to-date analysis of how subject-matter experts perceive and address cyber-risks in a more digitized world.

Expanded Scope of Biases: While the original paper focused on *optimism bias* and *illusion of control*, this research takes a more comprehensive approach by including *overconfidence* and the *availability heuristic*. This expanded examination of cognitive biases in cyber-security risk perception enhances the understanding of decision-making processes in this field, adding depth to the existing research.

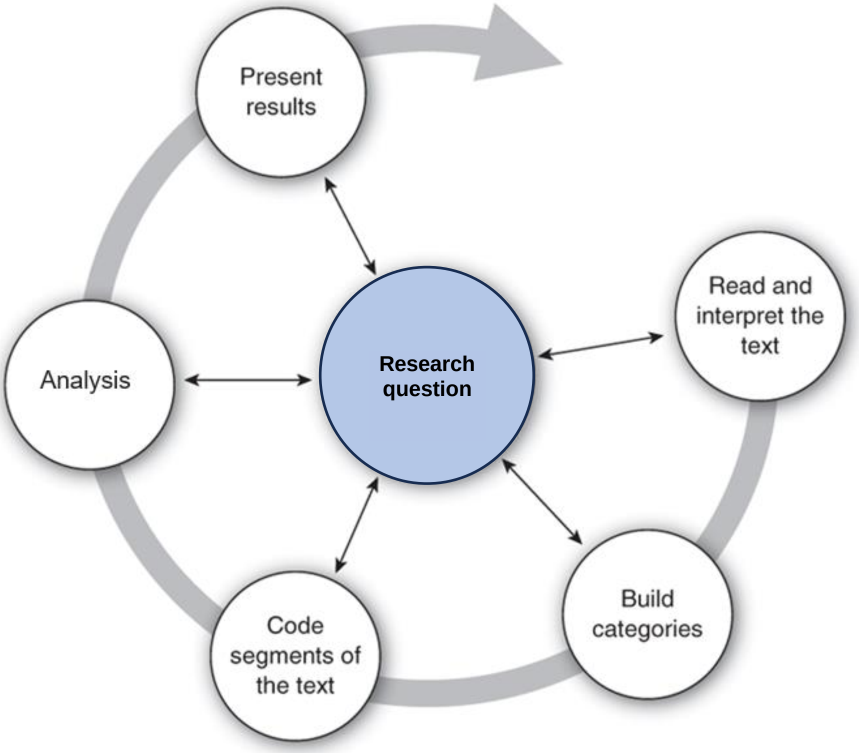
Impact of Organizational Practices: In extension of the underlying paper, this research aims to explore further relationships between cognitive biases and organizational practices, including reporting structures, procedures such as audit practices and crisis communication plans, and fire drills. Investigating these aspects could offer valuable insights into their implications for cyber-security effectiveness and decision-making.

This dissertation aligns with the aspect of strategic decision making under bounded rationality (Das & Teng, 1999; Eisenhardt & Zbaracki, 1992; Schwenk, 1984; Schwenk, 1986) and uncertainty (Fielder et al., 2018; Gomez & Villar, 2018; Tversky & Kahneman, 1974; Tversky & Kahneman, 1992) as well as the decision-making process as it relates to digital technology (Tamm et al., 2014). In addition, this thesis addresses some of the future research questions proposed by Alsharida et al. (2023) such as how psychological factors, including cognitive biases, shape cyber-security behaviors as well as which factors cause an increase or decrease in cyber-security motivation toward emerging technologies. Moreover, this work examines human and organizational aspects and patterns that lead to distortions in the decision-making process (cf. Nuijten et al., 2020) while drawing on the organizational evolution of the CISO role (Hooper & McKissack, 2016; Lowry et al., 2022; Maynard et al., 2018; Rothrock et al., 2018). Lastly, this reserch aligns with the direction suggested by Jalali et al. (2019), aiming to uncover valuable insights into the inherent biases present in managerial decision-making processes concerning cyber-security and extends the work of Ceric and Holland (2019), who utilized secondary sources and recommended additional investigation into biases related to cyber activities, given the crucial and unpredictable role of human factors in such processes.

In expansion of the brief methodological overview provided in Chapter 1.5, this section offers a detailed account of the research framework employed in this study. The research utilized a mixed-methods approach, combining qualitative and quantitative methodologies to comprehensively examine the subject matter. Given the evolving nature of cybercrime and its wide-ranging implications, an interdisciplinary framework was adopted, integrating insights from economics, social sciences, political science, and computer science. This approach enriched the analysis of complex issues and aimed to significantly contribute to the academic literature on cyber-security.

The qualitative phase began with an extensive literature review, drawing from academic journals utilizing databases such as EBSCOhost, JSTOR, and ERIC, alongside industry reports, government publications, and reputable media sources. This foundational work identified key areas for further investigation. To validate and narrow down these preliminary findings, four background interviews were conducted with renowned experts in cyber-security, cyber-risk, and data privacy. The interviews were analyzed using Kuckartz's (2014) structured content analysis approach, which identified *optimism*, *overconfidences*, and the *availability heuristic* as common themes in decision-making within cyber-security. The staged downselection of biases was integrated into this phase, ensuring that the focus remained on the most impactful biases. These themes provided critical insights that contextualized the literature review (see Figure 14).

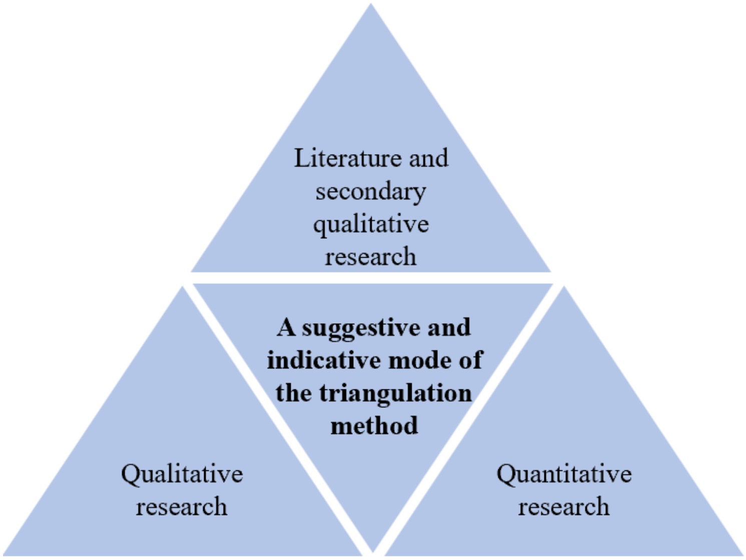
Figure 14: Structured Content Analysis



Source: Adapted from Kuckartz (2014)

This analysis, conducted with the assistance of MAXQDA software, employed a combination of deductive and inductive reasoning to develop a robust empirical study. Insights drawn from interviews with four distinguished experts, alongside a comprehensive review of the literature, were synthesized to inform the focus and content of the study's questionnaire. This iterative process ensured that the research was firmly grounded in both theoretical foundations and practical realities. The resulting questionnaire was carefully designed to capture the nuances of biases and decision-making practices within the cyber domain. After refining the questionnaire based on expert feedback, it was deployed to a high-quality sample of practitioners, including C-Suite executives. The quantitative data collected from this survey was then subjected to rigorous analysis using Structural Equation Modeling (SEM) and SPSS, allowing for the identification of patterns and relationships among key variables. The methodology, along with specific applications of SEM and SPSS, is elaborated upon in Chapter 6.5. This mixed-method approach provides both breadth and depth, combining qualitative insights with quantitative rigor. Although the sample was non-representative, limiting generalizability, the use of triangulation strengthened the research's credibility and dependability. As summarized by Brady and Collier (2010, p. xiv), the effectiveness of qualitative analysis is enhanced when combined with quantitative research, while quantitative analysis benefits greatly from being based on qualitative analysis and insights. By utilizing triangulation, a multi-method approach was employed to strengthen the credibility and dependability of the research outcomes (see Figure 15). This methodology not only ensures the validity of the findings but also enables a thorough and resilient analysis to be conducted.

Figure 15: Methodical Triangulation


Literature and secondary qualitative research
A suggestive and indicative mode of the triangulation method
Qualitative research
Quantitative research

Source: Adapted from Tzagkarakis and Kritas (2023)

6.3 Background Interviews

Four background interviews were conducted with subject matter experts to gather additional facts and incorporate their input into the development of the questionnaire. The five background questions asked in these interviews were grounded in both theoretical insights and empirical gaps identified in existing literature, crafted to explore key issues surrounding digital transformation, cyber-security, and human error within organizations. In separate face-to-face settings, the interlocutors were systematically asked these questions, applying process tracing and using an inductive approach to elicit deeper insights based on their real-world experiences while aligning with key themes in academic discourse.

There is a significant gap between CEOs' recognition of technology's strategic importance and the lower emphasis on cyber-security (e.g., Alsharida et al., 2023; Dal Cin et al., 2023). While organizations understand the importance of digital transformation, cyber-security is often seen as a technical issue rather than a strategic priority (Ament, 2017; Frank, 2020). The aim is to uncover factors contributing to this inconsistency, such as financial constraints, lack of cyber-security knowledge among decision-makers, and misaligned organizational priorities. Consequently, this brings up the first background question:

BQ1: Digital Transformation is one of the key themes keeping organizations busy. In a study of more than 1,000 CEOs, 96% acknowledge the critical role that technology plays in their strategy. At the same time, less than half of them (44%) see cyber-security as a strategic matter. What could be contributing factors causing this discrepancy?

Rapid technological innovation introduces potential risks, as research indicates that organizations often adopt new technologies without sufficient cyber-security assessments. According to EY (2021), 58% of CISOs admit that cyber-risks are not always fully assessed before implementation, exposing organizations to vulnerabilities. This aligns with other observations, suggesting that cyber-security is often seen as an afterthought (e.g., Dal Cin et al., 2023; Hielscher et al., 2023). As a result, this raises the second background question:

BQ2: Research suggests that the accelerated pace of technological innovation is a risk factor for cyber-attacks. Approximately 58% of CISOs indicate that their organizations occasionally adopt new technologies without adequate timeframes for conducting appropriate cyber-security assessments. What are possible causes for this observation?

Human error remains a key factor in data breaches, accounting for 88% of incidents (Hancock, 2022). Despite this, organizations struggle to implement effective safeguards against such errors, potentially due to gaps in training, culture, proactive planning, and the occurrence of various judgmental flaws (e.g., Alnifie & Kim, 2023; Alsharida et al., 2023), which is leading to the third background question:

BQ3: When it comes to cyber-security, humans are often labeled the "weakest link". In fact, research suggests that 88% of all data breaches can be routed to human error. Based upon your own experiences, why do you think organizations struggle to put appropriate safeguards in place?

Despite increasing cyber-threats, many CISOs feel their advice is not sufficiently heeded by leadership. This issue could stem from organizational silos, misaligned priorities, or a lack of integration between cyber-risk management and business strategy (Aiello et al., 2022; Hielscher et al., 2023; Loonam et al., 2022). This brings up the fourth background question:

BQ4: Cyber-threats have been proliferating in recent years. In a recent study, nearly half (43%) of CISOs report that they have never felt more worried to handle the ever-growing cyber-threat. What could be the reasons that they feel their advice is being disregarded?

High-profile incidents like the Colonial Pipeline ransomware attack in 2021 highlight a reactive approach to cyber-security. This reactionary approach, observed in other major breaches, highlights the tendency of organizations to take meaningful action only after a significant incident occurs (e.g., Ceric & Holland, 2019; Kianpour et al., 2019; Nikkhah & Grover, 2022; Ting, 2019). The final background question seeks to investigate why organizations delay critical cyber-security projects, potentially due to budget constraints, lack of regulatory pressure, or misjudged risks:

BQ5: Founded in 1962, Colonial Pipeline encountered a ransomware attack in 2021, causing wide-ranging fuel shortages across the United States' East coast over multiple days and bringing the U.S. President to the scene who declared a "state of national emergency". The incident created headlines around the world. Only afterwards, the company decided to hire the first CISO in the company's history. What could be the reasons that action was apparently only taken after the incident?

The development of these background questions followed a process tracing approach, aimed at uncovering the causal mechanisms behind observed discrepancies in cyber-security practices (Bennett & Checkel, 2014; George & Bennett, 2005). The questions were also informed by expert interviewing techniques as described by Trinczek (2009), which emphasizes an open, exploratory structure while maintaining alignment with the research objective. Following the methodological aspects of expert interviews outlined by each interview had a duration ranging from 30 to 60 minutes, thereby affording ample time and opportunity for the interlocutors to articulate their viewpoints and delve further into the discourse. The interviews were transcribed and subsequently analyzed. The interviews took place between November 2023 and March 2024, and involved the following subject matter experts (see Table 9).

Table 9: Interlocutors of Background Interviews

Interview	Name	Profile
1	Tim Wybitul	A prominent data protection lawyer engaged in advising both German and global corporations on intricate matters pertaining to data protection and cyber-security. He is a partner at the global law firm LathamWatkins (LW). With approx. 7,000 employees and US$5.5 billion in revenue, LW is deemed the world’s 2nd largest law firm. Tim Wybitul has authored numerous books on data protection and chairs LW’s global Data Privacy Committee. He has also provided expert testimony to the German Parliament on the evolution of data protection legislation in Germany.
2	Jens-Phillip Jung	CEO of Link11, an award winning and leading German Cyber-Security-as-a-Service provider with an extensive footprint across the critical infrastructure space with emphasis on Financial Services, Transport and Logistics, Utilities, and the Public Sector. With offices in Frankfurt, Tel Aviv and Vancouver, the company runs a 24/7 security operations center (SOC) and mitigates more than 100,000 cyber-attacks a year. *Full disclosure: The author of the dissertation previously served as Link11’s Chief Operating Officer from 2017-2022. The author declares no competing interests.*
3	Ralph Noll	A partner at the auditing firm Deloitte and head of the firm’s Cyber Risk practice in Germany. With approx. 415,000 employees and US$60 billion in annual revenue, Deloitte is considered the world’s largest management advisory and auditing firm. Ralph Noll is a Certified Information Systems Auditor (CISA) and certified as a data protection officer. His areas of responsibility include Cyber Resilience, Incident Response, Cyber Forensics, Cyber Investigations and Business Continuity Management.
4	Carsten Meywirth	Chief of the Cybercrime Division at the Bundeskriminalamt (BKA), Germany’s Federal Criminal Police Agency. With over 8,000 staff, the BKA coordinates federal and state police forces and investigates international crime, terrorism, and national security matters. The agency plays a key role in counterterrorism and represents Germany in Interpol and Europol. Carsten Meywirth, with a distinguished thirty-year career at the BKA, has held various leadership roles within the agency. He established the Cybercrime Division in 2020, focusing on high-profile investigations in the digital realm.

Each interlocutor was carefully selected based on three specific criteria: (i) With prominent roles in advisory and law enforcement, these individuals possess strategic insight and operational oversight in their respective fields. (ii) Each brings over 20 years of in-depth expertise in cybercrime, cyber-risk management, cyber-resilience, and data protection. (iii) The very nature of their respective roles gives them a wealth of exposure across industry sectors, companies, and cases, extending well beyond their own organizations.

Due to the extensive range of judgmental shortcomings discovered through the examination of existing literature, it became imperative to select a subset of these patterns for evaluation, considering that certain biases and heuristics hold greater significance in particular circumstances. Following the framework presented in Chapter 6.2, qualitative research methods were employed following Kuckartz (2014). A structured content analysis was conducted, and the data was coded using MAXQDA version 24.0.0 (VERBI Software GmbH, 2023), a software tool designed to cater specifically to the needs of qualitative and mixed methods research. The codebook is attached as Appendix 1. As a result of this approach, the list of biases and heuristics identified in comparison to the literature review has been significantly narrowed down. The insights gathered pointed toward the presence of several biases and heuristics including *optimism bias, overconfidence*, and the *availability heuristic*. These judgmental errors were consistently observed and frequently emerged as reoccurring themes across all four interviews conducted with the interlocutors. Consequently, emphasis has been placed on investigating these biases and heuristics to validate their existence in the field trial.

6.4 Questionnaire Survey

This section presents the design, execution, and analysis of an empirical survey targeting senior executives to gather data on cyber-security decision-making. Conducted online for practical and ethical reasons, the survey examines key factors influencing risk perception and response. The subsections detail the methodology, questionnaire design, and sample demographics, offering a comprehensive overview of the data collection process and its significance to the study's objectives.

6.4.1 Empirical Study

The empirical survey was conducted via an online portal, following a thorough evaluation of the advantages and disadvantages of various survey methods. This evaluation considered factors such as reach, speed, participant convenience, and ease of data entry, as outlined in previous research (Andrade, 2020; Evans & Mathur, 2005; Evans & Mathur, 2018; Nayak & Narayan, 2019). The decision to use an online survey was based on its ability to efficiently reach a large and diverse sample, facilitate rapid data collection, and offer convenience for participants, thereby minimizing barriers to participation. Considering the high-profile roles of many respondents and their busy schedules, online gave participants the discretion to choose where and when they answer the questions. The online format also streamlined data entry and analysis, reducing potential errors and saving time compared to traditional methods. This approach was selected after weighing these practical benefits against potential limitations, such as response rates and data security concerns, which were mitigated using secure and a reliable online survey platform. This method aligns with previous research methodologies in cyber-security. For example, Hewitt and White (2022) employed online surveys to explore *optimistic bias* in home computer security, and Hong et al. (2023) used a similar approach to examine the impact of work overload on cyber-security behavior. Kianpour et al. (2019) used a similar approach to study third-party cyber-risks, while van Schaik et al. (2020) investigated cyber-risk perception using online methods. Qu et al. (2019) further employed online surveys to explore decision-making in cyber-security measures. These studies collectively highlight the effectiveness and practicality of online surveys in cyber-security research, supporting its selection in this thesis.

Ethical considerations were crucial in this research. The online format ensured a higher level of confidentiality compared to face-to-face methods, especially considering the sensitive nature of the topic being explored. This approach helped reduce social desirability bias and encouraged more candid responses. To prevent multiple submissions, unique, one-time links were issued, anonymized, and discarded post-survey to ensure no personal data could be traced back to the respondents. To accommodate the linguistic preferences of participants and minimize language-related bias, the survey was available in both English and German. As the author is bilingual, the German translation was carefully conducted to ensure accuracy and maintain consistency across both versions. The survey was open from April 9 to July 26, 2024, allowing ample time for participation and data collection.

The importance of overcoming challenges related to low response rates and non-response bias among executive-level participants was emphasized in this research. The occurrence of low response rates in online surveys is a frequent phenomenon (Evans & Mathur, 2018; Fricker & Schonlau, 2002), especially as it relates to senior executives and the length of the questionnaire. Nonetheless, it remains a limitation of this study. The presence of non-response bias presents a significant challenge as it creates limitations in comprehending the findings of the complete sample when there are noticeable variations between those who responded and those who did not. Utilizing analysis of variance (ANOVA), the analysis results revealed no statistically significant discrepancies between early and late respondents in terms of the variables studied. While this outcome offers some assurance concerning non-response bias, it was noted that the likelihood of bias cannot be completely discounted. To further explore the potential existence of non-response bias, participants were questioned about how a material cyber-security incident would influence their willingness to engage in future surveys over the next 12 months. Surprisingly, no respondents indicated that such an event would substantially reduce their willingness to participate, with a single respondent out of 144 (0.69%) reporting a slight decrease. On the contrary, almost two-thirds (61%) stated that such a material cyber-security incident would not significantly affect their willingness to participate. Additionally, 38% of participants revealed that experiencing a material cyber-security incident could even enhance their willingness to engage in future surveys. This nuanced insight into participant attitudes contributes complexity to evaluating potential non-response bias, indicating diverse and potentially positive attitudes towards ongoing survey participation regardless of external circumstances.

6.4.2 Questionnaire Design

The questionnaire incorporates the finding of the background interviews and draws on the foundational research by Rhee et al. (2012), which focused on *optimism bias* and the *illusion of control* in cyber-security decision-making. Building upon their scales and methodologies, the questionnaire was adapted and expanded to encompass additional variables pertinent to cyber-risk perception. Specifically, the questionnaire explores the influence of experience within the field, organizational characteristics (such as organizational type, reporting lines, and past breach experiences), and factors like the presence of a pre-existing crisis communication plan, annual auditing practices, and regular fire drills. To identify possible patterns on organizational level, a more extensive range of questions has been utilized, enabling the application of multilevel factor analysis to draw inferences. These adaptations aim to provide a more comprehensive understanding of decision-making processes in cyber-security and contribute to the development of effective risk management strategies.

In practical terms, the questionnaire utilizes multiple-choice questions along a Likert-5 scale for simplicity and feasibility in data collection, with a total of 22 questions and a factor analysis comprising 17 items. This approach builds upon established scales and methodologies from Rhee et al. (2012) and extends the inquiry to broader dimensions of cyber-security decision-making. The questionnaire was validated by synthesizing findings from content analysis of background interviews and an extensive scientific literature review, following Lizarraga et al. (2009). These steps ensured that the questionnaire captured key influencing factors, reflecting both theoretical constructs and practical realities in cyber-security decision-making.

Through the utilization of a standardized questionnaire and calibrated instruments, the impact of information bias was mitigated while ensuring a consistent approach to data collection. That way, all participants were presented with identical questions, and the variables under investigation were measured consistently. Details about the composition of the constructs can be found in Chapter 6.5.1. A copy of the questionnaire has been added as Appendix 2.

6.4.3 Sample Demographics

To obtain the most meaningful and high-quality data, subject matter experts from companies with substantial expertise in detecting and defending against cyber-attacks were chosen, where business success is directly tied to resilience against such threats. The panel was meticulously recruited from existing clients of Deloitte within the countries of Germany, Austria, and Switzerland (commonly referred to as the D-A-CH region). The participants are not merely frontline staff or entry-level positions, but rather decision-makers in cyber-security, risk management, compliance, data privacy, and information technology (IT). The selection criteria prioritized senior executives, including Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), Chief Technology Officers (CTOs), Chief Digital Officers (CDOs), Heads of Risk Management, Heads of Compliance, and Heads of Information Technology. This data set is both rare and valuable, given the difficulty in accessing such high-level professionals and C-Suite executives who are typically busy and reluctant to participate in surveys or questionnaires.

Moreover, to increase the number of participants, efforts were made to involve the CISO Alliance (https://www.ciso-alliance.de/) and FINAKI (https://finaki.de/sekop2024/). The CISO Alliance is a non-profit association, an advocacy group, and a community platform for CISOs in Germany. On the other hand, FINAKI organizes the SEKOP conference annually, an event where cyber-security professionals from renowned user companies of all industries meet. Both organizations promoted the survey through their respective communication channels.

For ethical reasons, each of the participants had received an invite beforehand and expressed their will to participate in the survey. No incentive was provided apart from receiving information regarding the survey findings after the dissertation’s formal publication.

The panel included over 2,600 recipients, with 146 participating in the survey, resulting in a commendable 6% participation rate. After data cleansing, two responses were disqualified due to inconsistencies, reducing the final sample size to 144. This current sample size is only marginally smaller than the 204 participants in the original Rhee et al. (2012) study. The excluded responses were completed significantly faster than the average, suggesting they may have been hastily answered. Importantly, this exclusion did not materially impact the study's results. Insights from 144 CISOs and other cyber leaders in the D-A-CH region underscore the high quality and relevance of the data, enhancing the study's credibility and reliability. The survey participants consisted of a blend of individuals from medium-sized enterprises ("Mittelstand") as well as from large corporations spanning various industries (see Table 10).

Table 10: Demographics of Data Sample

Demographic Factor	No. of Participants (%)	No. of Participants (n)
Age cohort		
<30 years of age	2.08%	3
30-39 years of age	13.89%	20
40-49 years of age	28.47%	41
>50 years of age	55.56%	80
Gender		
Male	88.19%	127
Female	9.03%	13
Other	0.00%	0
Undisclosed	2.78%	4
Domain Experience		
<5 years	15.28%	22
>5 years	17.36%	25
>10 years	19.44%	28
>15 years	47.92%	69
Functional Area of Responsibility		
Information Technology	32.64%	47
Cyber-Security	26.39%	38
Risk, Compliance, Data Privacy & Data Protection	21.53%	31
Other	19.44%	28
Industry Background		
Financial Services	19.44%	28
Healthcare	3.47%	5
Manufacturing	14.58%	21

Professional Services	23.61%	34
Public Administration	6.25%	9
Transportation and Logistics	4.17%	6
Utilities	6.25%	9
Retail, Wholesale & Distribution	15.28%	22
Other	6.94%	10
Size of the Organization		
<500 employees	26.39%	38
500-5,000 employees	28.47%	41
5,001-10,000 employees	20.14%	29
>10.000 employees	25.00%	36

6.5 Data Analysis and Results

6.5.1 Structural Equation Model (SEM)

Building on the foundational work of Rhee et al. (2012), which utilized structural equation modeling with partial least squares (PLS-SEM), this research adopts a covariance-based structural equation modeling (CB-SEM) approach. While Rhee et al.'s study provided valuable insights using PLS-SEM, CB-SEM was selected for its robust theoretical framework and broader acceptance in the academic community (Byrne, 2010; Jöreskog & Sörbom, 1982). CB-SEM offers enhanced capabilities for evaluating complex relationships between observed and latent variables, providing overall model fit indices, and supporting hypothesis testing with test statistics and confidence intervals for parameter estimates (Dash & Paul, 2021).

This decision is further supported by previous research that employed SEM in similar contexts. For instance, Myburgh et al. (2015) demonstrated how SEM can effectively capture managerial decision-making self-efficacy, while Kianpour et al. (2019) utilized SEM to analyze the impact of social preferences and cyber-security attack experiences on organizational cooperation. Furthermore, Safa et al. (2015) and Hong et al. (2023) showcased SEM's versatility in modeling the effects of external factors and corporate ethics on cyber-security behavior. These studies collectively underscore SEM's strength in addressing complex constructs and interactions, reinforcing the suitability of SEM for this research. To address CB-SEM's assumptions of multivariate normality and sample size requirements, re-sampling techniques such as bootstrapping are utilized to ensure the robustness of the results (Tibshirani & Efron, 1993). The decision to utilize CB-SEM was reached after thorough deliberation on the sample size and the appropriateness of this methodology for the data. This choice was made in consultation with the Chair of Econometrics at the University of Gdańsk, ensuring that CB-SEM was suitable for the research context and objectives. The analysis itself was performed using SmartPLS v4 (SmartPLS GmbH, 2024).

Constructs

In extension of Rhee et al.'s (2012) approach, a revised method has been employed to combine the observable variables from questions 18-25 (see Appendix 2) to establish a construct that embodies *optimism bias*. Likewise, the observable variables from questions 26-35 have been merged to form a construct measuring *overconfidence bias*. Finally, the observable variables from questions 36-39 have been combined to create a construct evaluating the presence of an *availability heuristic*. Each of the three constructs serves as a latent variable. The initial questionnaire was considerably longer, reaching roughly 50 questions, which presented a significant burden for the executives it was intended for and would have further complicated the data collection process. To reduce these challenges, the number of questions was cut to 39, though this number was still considered lengthy. Consequently, the construct used to assess the *availability heuristic* was limited to only four observable variables, which resulted in lower statistical reliability compared to the other two constructs that were built upon eight and ten observable variables, respectively. This important tradeoff highlights the balance between obtaining comprehensive data and maintaining participant engagement, which is essential for attaining high-quality responses from executives. Bearing this in mind, this SEM model explores:

1. **Optimism Bias ("Optimism"):** This is the endogenous variable, representing the tendency to underestimate the probability of negative cyber-security events.
2. **Communication Plan ("Comms_Plan"):** This construct indicates whether the organization has a formal communication plan for cyber-security incidents. It is hypothesized to positively influence *overconfidence bias*, as the existence of a crisis communication plan may lead people to mistakenly believe they are adequately prepared.
3. **Overconfidence Bias ("Overconfidence"):** This construct reflects the participant's tendency to overestimate their own cyber-resilience. *Overconfidence bias* is hypothesized to influence *optimism bias*.
4. **Prior Attack Experience ("Attack"):** This construct measures whether the participant has previously experienced a cyber-security incident. It is hypothesized to negatively influence

optimism bias, causing participants to be more aware of potential risks and, as a result, less optimistic about the likelihood of avoiding future events.

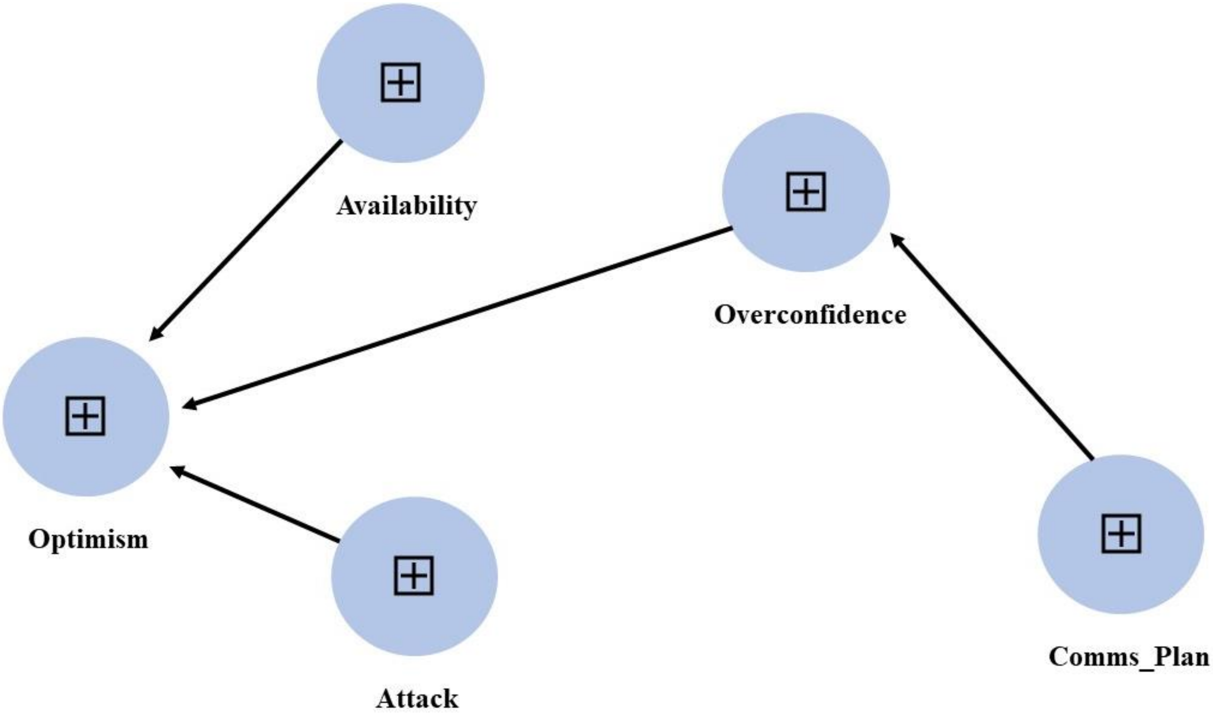
5. **Availability Heuristic ("Availability"):** This construct captures the extent to which easily recalled incidents (such as recent or highly publicized cyber-attacks) influence risk perception. It is also hypothesized to influence *optimism bias*.

Path Relationships

- **Comms_Plan → Overconfidence:** Increases *overconfidence bias* as people tend to think that having a crisis plan means they are well prepared, thereby elevating their confidence.
- **Overconfidence → Optimism:** Increases *optimism bias* due to an inflated sense of capabilities and resilience**.**
- **Attack → Optimism:** Previous exposure to an attack decreases *optimism bias*, increasing awareness of the reality and presence of cyber-threats.
- **Availability → Optimism:** Increases *optimism bias* due to reliance on easily recallable information.

The relationships of the constructs have been illustrated in Figure 16.

Figure 16: Path Relationships



6.5.2 Results

The SEM analysis yielded several significant relationships among the constructs. Notably, the parameter estimates, standard errors, T values, and P values for each path relationship provide insights into the influences on *optimism bias* within the cyber-security context.

Table 11: Path Coefficients (Unstandardized)

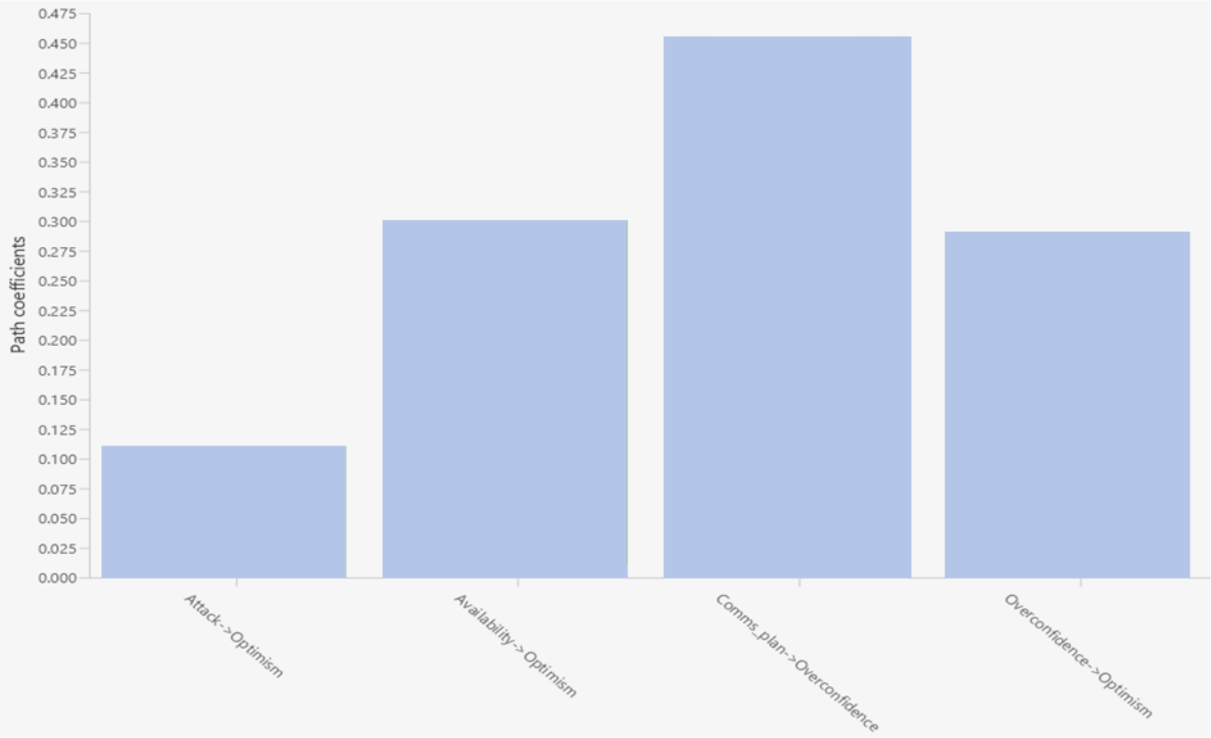
	Par. estimates	Stand. errors	T values	P values
Comms_Plan → Overconfidence	0.455	0.098	4.637	0.000
Overconfidence → Optimism	0.290	0.090	3.236	0.002
Attack → Optimism	0.111	0.037	3.004	0.003
Availability → Optimism	0.301	0.156	1.930	0.056

- **Impact of Comms_Plan on Overconfidence Bias:** The presence of a communication plan can greatly exacerbate *overconfidence bias*, potentially fostering a false sense of readiness, resulting in heightened levels of *overconfidence* among participants.
- **Impact of Overconfidence Bias on Optimism Bias:** *Overconfidence bias* significantly influences *optimism bias*, showing a strong positive relationship, where higher levels of *overconfidence* correspond to higher levels of *optimism bias*.
- **Impact of Prior Attack Experience on Optimism Bias:** Prior attack experience significantly influences *optimism bias*, with a positive relationship indicating that those with prior experiences of cyber-attacks tend to have higher levels of *optimism bias*. This occurrence, akin to the gambler's fallacy, leads individuals to believe that lightning will not strike twice, even though the statistical probabilities remain the same.
- **Impact of Availability Heuristic on Optimism Bias:** The *availability heuristic* has a moderate impact on *optimism bias*, suggesting that readily accessible information in the absence of recent cyber-attacks can contribute to higher levels of *optimism bias*.

Table 12: Path Coefficients (Standardized)

	Path coefficients
Comms_Plan → Overconfidence	0.428
Overconfidence → Optimism	0.310
Attack → Optimism	0.260
Availability → Optimism	0.226

Figure 17: Findings Relative to Path Coefficients



These findings highlight critical dynamics within cyber-security risk perceptions, specifically how prior experiences, readily available information and preparation efforts interplay to shape *optimism bias* and *overconfidence* as well as the presence of an *availability heuristic* among cyber-security professionals.

Coefficient of Determination

The R² values, also known as the coefficient of determination, indicate the extent to which the independent variables in the model account for the variability of the dependent variable.

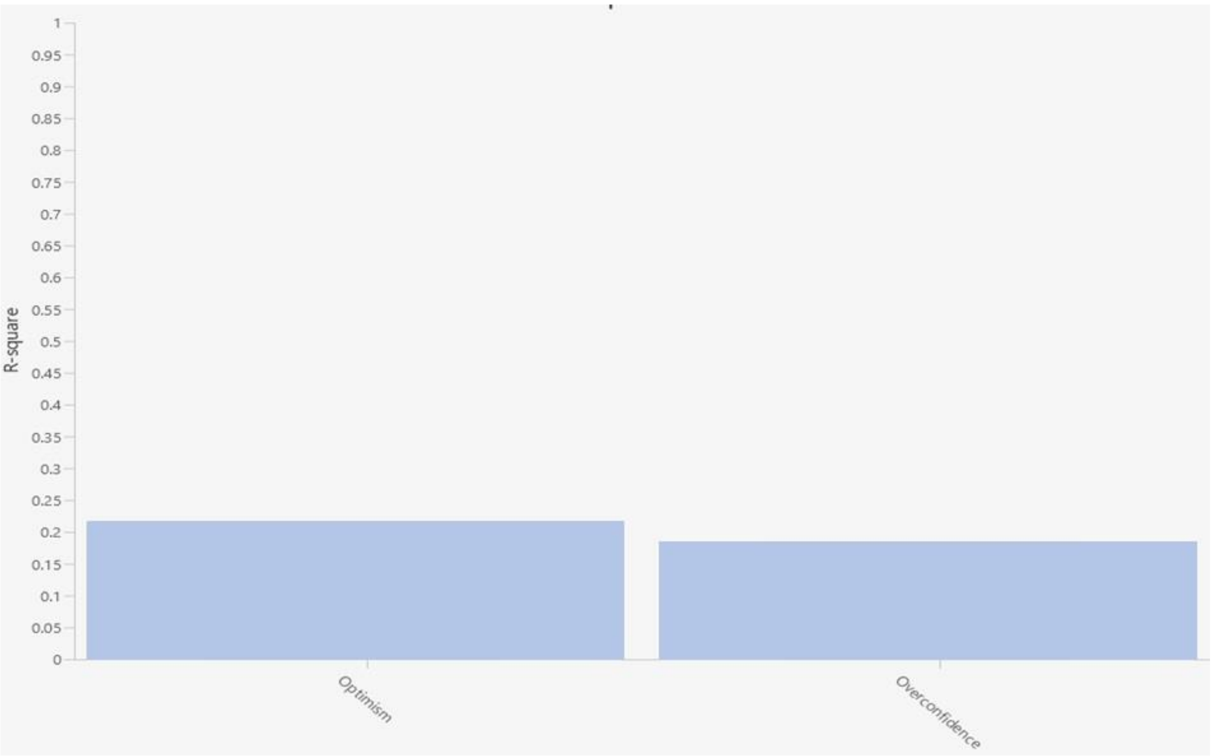
Table 13: R-Square

	R-square
Optimism	0.214
Overconfidence	0.183

- **Optimism** $(\boldsymbol{R^2 = 0.214})$**:** This indicates that 21.4% of the variance in Optimism is explained by the predictor variables (Attack, Availability, Overconfidence) in the model. It implies a moderate level of explanatory power.

- **Overconfidence** ($\boldsymbol{R^2 = 0.183}$)**:** This indicates that 18.3% of the variance in Overconfidence is explained by the predictor variable (Comms_Plan) in the model. This also suggests a moderate level of explanatory power.

Figure 18: R-Square



Both values suggest that while the model has a moderate explanatory power, other factors not in scope for this study may also contribute to the variance in these biases, presenting an area for further research.

Construct Reliability and Validity

Table 14: Construct Reliability and Validity

	Cronbach's alpha (standardized)	Cronbach's alpha (unstandardized)	Composite reliability (rho_c)	Av. variance extracted (AVE)
Attack	1.000	1.000	1.000	1.000
Availability	0.605	0.598	0.587	0.298
Comms_Plan	1.000	1.000	1.000	1.000
Optimism	0.852	0.854	0.859	0.463
Overconfidence	0.864	0.862	0.862	0.394

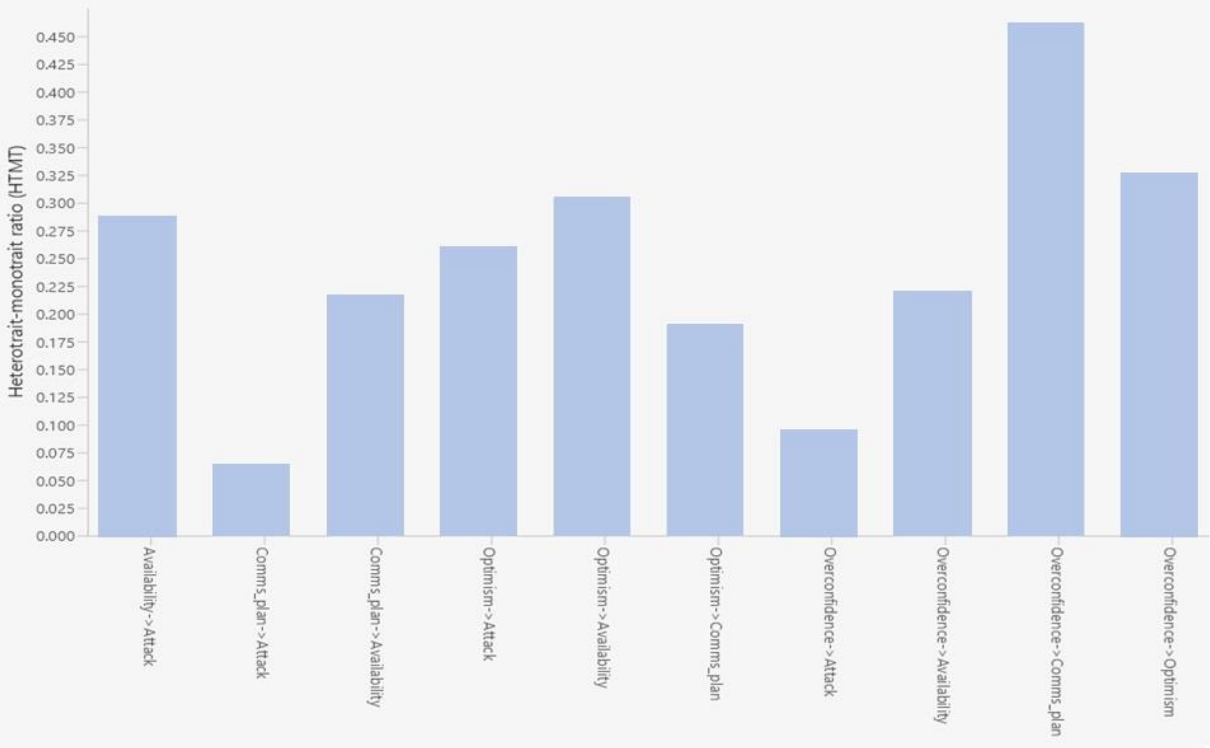
The Heterotrait-Monotrait ratio (HTMT) is a measure used to assess the discriminant validity of constructs in SEM models. Discriminant validity indicates the extent to which a construct is truly distinct from other constructs by not correlating too highly with them.

Table 15: HTMT Ratio

	Attack	Availability	Comms_Plan	Optimism	Overconfidence
Attack					
Availability	0.287				
Comms_Plan	0.064	0.215			
Optimism	0.259	0.304	0.190		
Overconfidence	0.095	0.220	0.462	0.326	

Values below 0.85 or 0.90 are commonly deemed acceptable, signifying good discriminant validity. In this instance, all HTMT values fall below these thresholds, implying that the constructs within the model are unique and not excessively correlated. Empty cells in the correlation matrix and Fornell-Larcker tables are attributable to the fact that two constructs (Attack and Comms_Plan) were each measured by a single observable variable. In CB-SEM, constructs with only one indicator do not contribute to the computation of correlations in the same way as multi-indicator constructs, as there is no variance to measure across multiple items. This approach is often taken when the construct is either inherently singular (e.g., a binary event or a unique item) or when data constraints necessitate this simplification. However, this can lead to non-standard outputs or omitted values in statistical reports, as the software may not generate meaningful correlations or reliability metrics for single-item constructs. For thoroughness and the sake of completion, the Fornell-Larcker criterion is provided in Appendix 3, although more emphasis is put on HTMT ratios as they are more relevant for assessing discriminant validity in this context.

Figure 19: HTMT Ratio



Goodness of Fit (GoF)

The model fit indices for this study present certain challenges, particularly considering the specialized and limited sample size (n = 144). The Root Mean Square Error of Approximation (RMSEA) is 0.120, which, although exceeding the ideal threshold of 0.08, falls within an acceptable range for studies with smaller datasets. The Comparative Fit Index (CFI) and Tucker-Lewis Index (TLI) are below the recommended threshold of 0.90, with values of 0.663 and 0.626, respectively. These figures are influenced by the specific constraints of the target group, which comprises cyber-security leaders across Germany, Austria, and Switzerland—a specialized population with inherent limitations in size (see Chapter 6.4.3 for details). Despite these lower indices, the robustness of the model is supported by the Wald tests, which indicate that the parameter estimates are statistically sound.

Table 16: Goodness of Fit

Model Fit Indices	
Chi-Square Test (χ^2)	700.017
Root Mean Square Error of Approximation (RMSEA)	0.120
Comparative Fit Index (CFI)	0.663
Tucker-Lewis Index (TLI)	0.626

Supplementary ANOVA Analysis

To further substantiate the SEM model's findings and address the challenges posed by its fit indices, a one-way ANOVA analysis was conducted, using SPSS version 21 (IBM, 2021). ANOVA was chosen for its ability to compare the means of three or more independent groups to assess the impact of categorical factors—such as audit practices, fire drills, and reporting lines—on constructs like *overconfidence* and *optimism*. ANOVA is particularly useful in this context as it tests for statistically significant differences between group means and can handle the comparison of multiple groups simultaneously. Key characteristics of ANOVA include its assumptions of homogeneity of variances and normality of data within groups, which were verified to ensure the robustness of the results. The one-way ANOVA approach was appropriate here, as it focuses on the effect of a single independent variable on the dependent variables.

The analysis revealed significant relationships between audit practices, fire drills, and biases such as *overconfidence* and *optimism*, reinforcing the trends identified by the SEM model. Although the SEM model's fit indices (RMSEA and CFI/TLI) suggested limitations, likely due to sample size constraints paired with the availability construct relying on only four observable variables, the ANOVA results validate and support the robustness of the identified relationships. These supplementary findings underscore the importance of the identified factors and suggest that, despite the model fit challenges, the study's conclusions remain statistically sound and relevant for future research. Further details are provided in Appendix 4.

Audit Practice: The annual external audit practices reveal a significant link between formal audits and *overconfidence* in cyber-security (p = 0.006). Among 144 participants, 52% reported formal audits with mandatory actions, 39% engaged in semi-formal audits, and 9% had no external audits. The correlation suggests that structured audits may lead to overestimating cyber-security capabilities. In contrast, factors like *availability* (p = 0.480) and *optimism* (p = 0.140) showed no significant impact from audit practices. These findings emphasize the need for organizations to remain cautious about inflated confidence, even with formal audits, to accurately assess vulnerabilities and risks.

Fire Drills: The analysis revealed a significant relationship between the practice of regularly conducting fire drills and simulating responses to large-scale cyber-attacks and *overconfidence bias* (p ≈ 0.000007). Notably, 65% of respondents indicated that their organizations do not conduct these exercises regularly. This absence of regular drills is an interesting observation, potentially contributing to an inflated sense of confidence in handling a cyber-security incident. This scenario points toward an *optimism bias*, where respondents might underestimate the likelihood of a cyber-attack, leading to insufficient preparation. Consequently, this *optimism bias* can result in an overestimation of cyber-resilience among those not regularly engaging in simulations. While the relationship between these drills and *optimism* approached significance (p = 0.0619), no significant effect was observed on *availability heuristics* (p = 0.3534). However, as previously discussed, this absence of significance may partly stem from the construct's reliance on a smaller set of observable variables. These findings underscore the risks of underestimating cyber-threats and emphasize the importance of regular preparedness to mitigate *overconfidence* and enhance risk management.

Reporting Lines: Notably, 47% of participants confirmed that the CISO reports to a technical leader, such as the CIO or CTO (see Appendix 5). In line with findings from other studies, this not only implies that cyber-security is still often seen as an IT responsibility but also highlights the importance of examining how organizational structure influences *overconfidence bias* in cyber-security leadership. When participants were subsequently grouped into Tech (n = 76) versus non-Tech (n = 68) categories based on the CISO's reporting line—whether they report to a Technology leader (such as the CIO or CTO) or to another, non-Technology leader in the C-Suite—the near-significant result for *overconfidence* (p = 0.0812) raises intriguing possibilities. This finding suggests that *overconfidence bias* might be influenced by the CISO's reporting structure, potentially reflecting differences in decision-making or risk assessment between those reporting to technical versus non-technical leaders. CISOs reporting to non-Technology leaders might be required to engage more in System-2 thinking—deliberate and analytical reasoning—due to the need for greater "translation" when communicating complex cyber-security issues. Interacting with a non-Technology leader who may think and communicate differently could compel the CISO to clarify and justify their strategies more rigorously, thereby affecting their confidence levels. Although the p-value is not statistically significant, it is closer to significance than other variables, indicating a trend worth exploring. The possibility of a Type II error should be considered, as a larger sample might have revealed a significant relationship. This emphasizes the need for further research to clarify this potential connection.

Key Findings

Empirical Insights into Cognitive Biases and Cyber-Security Practices: The empirical results provide important insights into the role of cognitive biases in shaping cyber-security practices, though they also highlight the complexity of these relationships.

Overconfidence Bias and Its Impact on Optimism Bias: The significant influence of *overconfidence bias* on *optimism bias* (β = 0.290, p = 0.002) confirms that an inflated sense of one's own cyber-resilience contributes to a skewed perception of risk. Moreover, the hypothesis that the presence of a communication plan increases *overconfidence* (β = 0.455, p < 0.001) is confirmed, suggesting that this might lead to an inflated sense of preparedness. Furthermore, this study reinforces that *optimism* does not mean individuals think negative events will never happen, but rather that they believe these events are less likely to happen to them. *Optimism bias* significantly reduces perceived risk, leading to decreased engagement in cyber-security behaviors. This leads to the belief that cyber-security practices are more important for others or organizations seen as more at risk. This is evidenced by the significant path coefficients in the empirical results (β = 0.45, p < 0.01).

Prior Attack Experience and Its Paradoxical Influence: While the data suggests that prior attack experience significantly influences *optimism bias*, with a path coefficient of 0.111 (p = 0.003), the direction of this influence is somewhat counterintuitive. One might reasonably hypothesize that experiencing a prior attack would reduce *optimism bias* by increasing awareness and caution. However, the findings indicate the opposite effect, where prior attack experience appears to increase *optimism bias*, potentially leading individuals to believe that another event is less likely, thus reducing perceived risk and vigilance. Therefore, the hypothesis that prior attack experience would negatively influence *optimism bias* is rejected.

Literature Support and Contradictions: The underlying paper by Rhee et al. (2012) provides foundational insights into this issue, demonstrating that increased cyber-security awareness among staff and managers can lead to an *optimistic bias*. This finding is supported by Hewitt and White (2022), who demonstrated that users who perceive a high likelihood of facing cyber-attacks often engage in riskier behaviors due to their underestimation of actual threats. These results align with the notion that heightened awareness does not necessarily improve risk perception but can foster *overconfidence bias*. Dillon and Tinsley (2016) further support this by showing that individuals who experienced a prior near-miss incident without severe consequences are less likely to adopt additional precautions compared to those who have faced more severe negative outcomes. Similarly, Alnifie and Kim (2023) revealed that *optimism bias* significantly influences cyber-risk exposure, leading to increased complacency and reduced protective actions.

Moreover, Kostyuk and Wayne (2020) highlight that awareness of cyber-security and secure online practices is generally low. Their findings suggest that while personal data breaches can elevate risk perception and promote safer online behaviors, their overall impact is often limited, resulting in substantial resistance to changing established online habits. This aligns with the view that awareness alone may not be sufficient to mitigate *optimism bias* and promote effective risk management.

Nuanced Perspectives on Awareness and Risk Behavior: Nevertheless, it is important to approach these findings with caution, as other research presents a more nuanced picture. Fatoki et al. (2024) showed that while awareness might foster some *overconfidence*, it can also play a protective role by mitigating risky behaviors. The authors propose that cyber-security awareness negatively moderates the relationship between attitudes toward cyber-security and risky behavior, suggesting that greater awareness, although potentially increasing *optimism*, can also reduce the likelihood of engaging in risky actions. Nonetheless, while Fatoki's results suggest that awareness can reduce risky behaviors, Eling and Jung (2024) imply that *optimism bias*, driven by self-protection and loss aversion, may still lead to insufficient investment in cyber-risk management measures.

Complex Interactions and Demographic Variations: These varying findings underscore the complex and sometimes contradictory effects of awareness and prior experiences on *optimism bias* in cyber-security. They highlight the need for further research into how the various factors interact to influence decision-making in cyber-security to fully understand these dynamics. Additionally, variations in the respective data sets may lead to slightly divergent results, particularly when considering the influence of distinct demographics, which may place varying levels of emphasis on users, operational staff, and senior leadership.

Availability Heuristic and Model Fit Analysis: The hypothesis that the *availability heuristic* affects *optimism bias* is marginally supported ($\beta = 0.301$, $p = 0.056$), indicating that while easily recalled incidents have some impact on *optimism bias*, this effect is not strong enough to be conclusive. Despite the significant relationships and the high quality of the data, model fit indices suggest areas for improvement, with RMSEA at 0.120, CFI at 0.663, and TLI at 0.626. Achieving a higher GoF might have been possible through model simplification. However, such simplification would have involved a significant trade-off by excluding additional critical variables and nuances crucial for understanding cyber-security decision-making. This highlights the balance between model complexity and GoF, given the sample size ($n = 144$). However, prioritizing data quality over quantity was essential, as the study included many difficult-to-attain senior executives, including top-level decision-makers, providing a robust foundation for the findings.

Discrepancy Between Perception and Action in Cyber-Security: An intriguing observation from the raw data reveals a discrepancy between perceptions of cyber-security importance and the actions taken. Over half (52.8%) rate their board's cyber-security knowledge as good or excellent (see Appendix 6). However, this self-assessed high level of knowledge may reflect *overconfidence* rather than an accurate appraisal of expertise. Such overplacement and overestimation of one's own abilities align with the findings on *overconfidence bias*, which significantly influences *optimism bias*.

The Bimodal Distribution and Availability Heuristic: A notable contradiction has emerged from the raw data. While 78.5% of respondents report that their CEOs view cyber-security as critical or extremely critical, a significant portion (45.1%) struggles to justify increased investments in cyber-security in the absence of recent attacks. This indicates that the group facing difficulties in justifying these investments represents the largest segment. This bimodal distribution suggests that decision-making is heavily influenced by the *availability heuristic*, where the emphasis is placed disproportionately on recent events. This cognitive bias, combined with an *overconfidence* in the organization's ability to withstand cyber-attacks, likely contributes to a complacent attitude toward proactive investment in cyber-security measures.

Supporting Evidence from Literature: These findings outlined above also align with Dong et al. (2021), who showed that when overconfident CIOs underestimate the seriousness of a cyber-security incident, they may be less likely to make adequate investments in gaining cyber-resilience. Their research also indicated that *overconfidence* suppresses the positive effects of other factors on cyber-security performance, resulting in poorer outcomes than expected. The raw data observations reveal a discrepancy between perceived and actual cyber-security practices, highlighting *overconfidence* and *availability heuristics*. This aligns with the broader findings and underscores the need for more accurate risk assessments and investment in cyber-security measures.

Reporting Structures: To substantiate and validate the study's conclusions, ANOVA was conducted as an additional analysis. The ANOVA results support the robustness of the SEM findings and provide further insights into the data, complementing the initial SEM analysis. The near-significance of *overconfidence* ($p = 0.0812$) indicates that CISOs reporting to technical leaders may show higher *overconfidence* due to closer alignment and communication. Conversely, reporting to non-technical leaders, which may involve different types of interactions and possibly more System 2 thinking, is associated with lower *overconfidence*. This suggests that the nature of the reporting line influences the degree of *overconfidence* in cyber-security judgments.

Impact of Regular Fire Drills and Formal Audits: The ANOVA analysis also uncovered significant relationships between regular fire drills, formal audits, and *overconfidence*. The significant relationship between regular fire drills and *overconfidence* (p ≈ 0.000007) indicates that a lack of such exercises may contribute to inflated confidence, potentially driven by *optimism bias*. On the other hand, the data indicates that formal audits, rather than reducing *overconfidence*, may be linked to higher levels of *overconfidence* (p = 0.006). This suggests that while formal audits are common, they may not be effective in mitigating *overconfidence* and might even contribute to an inflated sense of security. Thus, organizations should not only conduct regular fire drills but also critically assess their audit practices and ensure a realistic evaluation of their cyber-security posture.

Addressing Cognitive Biases for Better Cyber-Resilience: Overall, these findings highlight the impact of cognitive biases, shaped by organizational practices and leadership, leading to poor investment decisions and reduced cyber-security engagement. Addressing these biases through simulations, robust audits, and a critical assessment of reporting structures is crucial for improving cyber-resilience.

6.5.3 Limitations

This study intentionally focuses on the D-A-CH region, addressing a specific research gap within German-speaking countries. While this regional focus is valuable, it may limit the applicability of the findings to other geographical areas, so caution should be exercised when generalizing results beyond the D-A-CH region.

The sample size, although encompassing a diverse range of organizations from various industries and sizes across the D-A-CH region, may still be insufficient for drawing definitive conclusions across all variables studied. This limitation is reflected in the statistical model fit indices, where the RMSEA, CFI, and TLI are below ideal thresholds. The small sample size, despite the high-caliber participants and the specialized nature of the target group, coupled with the *availability* construct relying on only four observable variables, likely contributed to the lower fit indices. This suggests that while the parameter estimates are statistically sound, the overall model may not fully capture the complexity of the studied relationships. Consequently, the weaker model fit suggests that caution is needed when interpreting the results, as the statistical robustness is somewhat constrained by the inherent limitations of the sample. Exploring model re-specification or simplifying the model might help improve fit indices, but this must be balanced with the need to retain essential constructs.

The purposive sampling method, which selects participants based on specific criteria, could introduce bias and result in an unrepresentative sample of the broader population of cyber-security professionals. Given that 45% of participants represent companies with more than 5,000 employees (see Table 10), it is important to recognize that external audits are commonplace, particularly in large and regulated organizations across the D-A-CH region. Nonetheless, the potential bias should still be noted, as it could slightly skew the findings, especially if certain industries or organizational types are over- or under-represented. Additionally, results could be skewed since multiple responses from participants within the same organization were possible. It is important to note that the research focused on cyber-security professionals, not their organizations**.** This potential bias may also affect the statistical model's parameters, further contributing to the challenges in achieving a better model fit.

The study's reliance on self-reported survey data introduces additional potential biases that could affect the accuracy of the findings. The cross-sectional nature of the study captures data at a single point in time, which does not account for long-term trends or changes in cyber-security practices. These temporal limitations, coupled with the potential biases in self-reporting, may also impact the stability and generalizability of the model's findings. To address non-response bias, Question 15 was included to explore the impact of recent cyber-security incidents on respondents' future survey engagement. Despite this effort, the response rate of roughly 6% means that non-response bias cannot be fully eliminated. Additionally, selection bias is another concern, as executives who have faced severe negative outcomes, such as job loss due to cyber-security failures, might be less likely to participate. This could lead to a skewed perception of risk among respondents, influencing the statistical model's estimates and contributing to the lower fit indices observed.

The under-representation of women and younger individuals in this study is likely reflective of the current demographics within the cyber-security sector, particularly at senior levels. With nearly 90% of participants being male and more than half aged 50 and above, the sample mirrors the industry's skew toward older, predominantly male professionals, especially in senior leadership roles. This demographic composition may have influenced the statistical model's performance and could limit the generalizability of the findings. While this under-representation is a logical consequence of the sector's current makeup, it nonetheless constrains the ability to explore gender- or age-specific differences in cognitive biases. If future research aims to investigate these differences, a broader and more diverse data set would be essential. Expanding the sample to include a wider range of demographics, such as younger professionals and women, would provide a more nuanced understanding of how these factors influence the presence and impact of biases in cyber-security decision-making. Reducing the emphasis on leadership positions in sampling could also mitigate demographic biases, leading to a larger sample that more reflects a broader population of cyber-security professionals.

CONCLUSIONS

Research Questions

RQ1: When it comes to cyber-related questions, what are the cognitive biases that hinder subject matter experts in their decision-making and possibly lead to suboptimal outcomes?

As analyzed in Chapters 1 and 2, research has pointed out that there exist approximately 180 cognitive biases and heuristics that can impede decision-making processes. Following an informed down select applying qualitative research, this study has examined three of these judgmental errors: *optimism bias*, *overconfidence bias*, and the *availability heuristic*. The empirical findings discussed in Chapter 6 provide insights into how these biases influence decision-making among cyber-security experts, revealing their complex interplay between technical and human contexts. Specifically, the study found the following:

1. **Optimism Bias:** Decision-makers often underestimate the likelihood of adverse events, believing that such risks are less likely to affect them compared to others. This *optimism bias* leads to a lax approach to cyber-risk management.
2. **Overconfidence Bias:** Experts tend to overestimate their organization's cyber-resilience, resulting in inadequate precautionary measures and a false sense of security.
3. **Availability Heuristic:** There is a tendency to rely too heavily on recent or memorable incidents, which distorts the perception of cyber-risk and affects strategic responses.

The SEM model highlights how these biases interact, demonstrating that even experienced professionals, despite their extensive knowledge, are vulnerable to cognitive distortions that undermine cyber-resilience. This aligns with findings from Dong et al. (2021), which show a higher degree of *overconfidence* among executives compared to the general population. These observations go against the notion that individuals, when given enough information, would implement the necessary precautions. Such a dichotomy, grounded in cognitive distortion or misjudgment, leads to a laxer approach to risks and ultimately weakens organizations' cyber-security posture. The findings suggest that frequent external audits may correlate with increased *overconfidence* in cyber-resilience, as these practices might foster a false sense of security. The analysis of the *availability heuristic* shows a slight effect on *optimism bias*, indicating that while this cognitive shortcut influences *optimism*, its impact is not definitive. The results are supported by a bimodal distribution in the raw data: 78.5% of participants report their CEOs view cyber-security as a top priority, yet 45.1% find it challenging to justify increased investment in the absence of recent incidents. This disparity shows how reliance on recent events can distort risk perceptions and foster an unwarranted sense of security. While bias in judgment and decision-making is common, it is also manageable. Organizations can implement measures to reduce their likelihood, leading to better outcomes. The strategies highlighted in this research do not cover all possible approaches, yet they are intended to offer a strong foundation to build upon. Striving for absolute security is unrealistic, but insights from high-stakes environments like aviation or oil and gas industries can offer valuable lessons for improving operational excellence. Despite numerous technological advancements, it is undeniable that enhancing cyber-security and the efficacy of measures is heavily dependent on comprehending the human element. In line with findings from other studies, this further reinforces the notion that humans are the "weakest link" in cyber-security defenses. Furthermore, this research shows that human behavior is indeed influenced by bounded rationality, which contradicts the principles of traditional economics that assume humans are completely *rational agents* solely driven by the goal of maximizing their *utility*.

Future studies should explore additional cognitive biases beyond those covered in this research, examining how they specifically impact decision-making in various cyber-security contexts. Research could also investigate the effectiveness of targeted training programs designed to mitigate these biases and improve decision-making in cyber-security.

RQ2: What are the driving forces behind the proliferation of cyber-threats, and how do cognitive biases shape the effectiveness of countermeasures in the evolving cybercrime landscape?

As summarized in Chapter 1, while offenses like burglary and assault are more visible, cybercrime often operates in obscurity, leading to an underestimation of its impact and the risk of victimization. This issue has exacerbated since the COVID-19 pandemic due to increased online activity, which has fueled cybercriminal activities. This underestimation might contribute to the presence of an *availability heuristic* and *optimism bias*, where the relative invisibility of cybercrime compared to more tangible crimes results in its perceived lower risk. Chapter 3 examined the evolution of cybercrime, emphasizing how technological advancements have facilitated new business models such as CaaS. Building on this foundation, Chapter 4 explored the various types of threat actors, the infrastructure that supports their activities, and the key factors driving the proliferation of cybercrime. Chapter 5 further examined the dual nature of digital technology, emphasizing its role in broadening the attack surface while simultaneously exposing new vulnerabilities. This chapter explored the *spillover effects* of digital technology and its impact on cyber-risk, particularly how the expanded attack surface and vulnerabilities in critical infrastructure exacerbate cyber-security issues. Empirical research presented in Chapter 6 assessed the effectiveness of current countermeasures and identified how cognitive biases, such as *optimism* and *overconfidence,* undermine these efforts. The findings revealed that these biases often create a false sense of security and preparedness, which can lead to underinvestment in cyber-resilience. The conclusions are as follows:

1. **Cybercrime Dynamics and Technological Impacts:** The study highlights that the proliferation of cybercrime is driven by lowered entry barriers due to models like CaaS and widespread digital technology adoption. The persistence and evolution of Dark Web platforms underscore the resilience and adaptability of threat actors.
2. **Geopolitical and State-Sponsored Influences:** The research also points to the role of geopolitical tensions and state-sponsored activities in shaping cyberspace. Nation-states increasingly employ cyber capabilities for political and strategic purposes, blending traditional organized crime with state-backed operations. However, it remains evident that most cyber-attacks are perpetrated by individuals driven by financial incentives.
3. **Underestimation and Cognitive Biases:** A significant insight is the frequent underestimation of cybercrime's professionalism and industrialization, which fosters a false sense of security among organizations. This underestimation, coupled with cognitive biases such as the presence of *availability heuristics, optimism* and *overconfidence*, leads to inadequate preparation and investment in cyber-security.
4. **Strategic Implications:** The findings align with the principle of understanding one's adversaries as emphasized by Sun Tzu, one of the founding fathers of military strategy. They stress the need for a comprehensive understanding of cybercriminal tactics and the continuous assessment of one's security posture to foster proactive decision-making and enhance cyber-resilience.

While the study has elucidated several factors driving the proliferation of cyber-threats and the role of cognitive biases, future research should delve into the evolving tactics of cybercriminals to better inform threat models and countermeasures. This is especially important as the threat landscape continues to evolve.

RQ3: How are the economic consequences of cyber-security incidents underestimated due to cognitive biases, and what are the broader implications for businesses and societal resilience?

This thesis addresses the underestimation of the economic consequences of cyber-security incidents and their broader implications through a comprehensive analysis. In Chapter 3, the research established a foundation by examining the development of cybercrime, highlighting the emergence of business models like CaaS. It also addressed the challenges associated with accurately evaluating the *externalities* resulting from cybercrime, compounded by a substantial dark figure, indicating that numerous offenses may go unreported. Chapter 4 revealed that activities in the Dark Web are characterized by significant industrialization and professionalism, involving intricate criminal value chains. It highlighted the existence of an entire industry that provides "grey infrastructure" to facilitate these illicit activities. Most of these providers conceal their operations and operate in the shadows to evade law enforcement. Chapters 5 provide a range of examples of specific ransomware campaigns and the enormous damage they have caused. Numerous case studies are highlighted across various industries and sectors. A comprehensive summary is provided in Chapter 6, contextualizing how these costs have escalated over time and how the enactment of new privacy legislation is likely to cause damages to continue climbing. Moreover, empirical research presented in Chapter 6 assessed the effectiveness of current countermeasures and identified how cognitive biases, such as *optimism*, *overconfidence*, and the *availability heuristic* undermine the efforts to gain cyber-resilience. The findings revealed that these judgmental flaws often create a false sense of preparedness, which can lead to underinvestment in cyber-resilience. In essence, the conclusions are as follows:

1. **Economic Impact and Underestimation**: The substantial economic impact of cyber-security incidents is frequently underestimated. Data breaches, often driven by human error, can result in average costs of around US$4.3 million. High-profile cases have demonstrated that costs can quickly escalate beyond US$100 million, depending on the severity of the incident. These findings reinforce that organizations often face severe consequences due to inadequate preparation and poor decision-making, underscoring the need for accurate risk assessment and comprehensive security measures.
2. **Organizational Preparedness and Cognitive Biases**: Organizations face the inevitability of cyber-attacks, shifting the focus from *"if"* to *"when"* such an incident will occur. Adequate preparation, strategic planning, and rigorous testing for cyber-

security incidents are essential for all businesses, regardless of size. Organizations that take cyber-risk lightly and delay implementing measures often find themselves unprepared and vulnerable when incidents occur. The longer the recovery phase, the more severe the consequences (see Figure 13: Cyber-Resilience CurveFigure 13). *Overconfidence, optimism bias,* and reliance on *availability heuristics* often undermine efforts, leading to poor decision-making and increased vulnerability.

3. **Broader Implications and Regulatory Measures**: In today's interconnected world with intertwined value chains, the risks of *spillovers, free-rider effects,* and *moral hazard* are amplified. Much like a roped team in mountain climbing, where the failure of one climber can trigger a chain reaction, even a forward-thinking company that invests heavily in cyber-security remains vulnerable if its suppliers, customers, or other ecosystem partners experience a cyber-security incident. This scenario fosters *free-rider effects,* where entities benefit from others' cyber-security efforts without contributing, and *moral hazard,* where greater risks are taken because the costs are likely to be borne by others. The resulting ripple effects extend beyond immediate financial damages, affecting multiple facets of society and the economy. Critical infrastructure is particularly at risk, with the potential for extensive damage and cascading effects, such as blackouts. Effective measures, including robust regulatory frameworks and unified standards, are essential for combating cybercrime and mitigating economic damages.

Future studies should explore the long-term economic impacts of cyber-security incidents and how different industries respond to these challenges. Research could also investigate how improved risk assessment methodologies can help organizations better understand and mitigate the economic consequences of cyber-threats.

Theoretical Contribution

This research has significantly advanced the theoretical understanding of cyber-security, particularly by addressing key gaps and expanding existing frameworks.

1. **Extension of Cognitive Bias Theories in Cyber-Security:** This study extends existing theoretical frameworks by incorporating additional judgmental errors, such as *overconfidence* and the *availability heuristic,* into the analysis of cyber-security risk perceptions. Expanding on Rhee et al.'s (2012) focus on *optimism bias* and the *illusion*

of control, this research broadens our understanding of how various cognitive distortions influence the decision-making processes of cyber-security professionals, offering a more comprehensive theoretical framework for assessing cyber-risks.

2. **Geographical and Temporal Contextualization:** A significant theoretical contribution of this research is the incorporation of geographical and temporal dimensions into the study of cyber-security biases. The study extends the analysis beyond the United States to include experts from the DACH-Region, addressing a notable gap in the literature. This broader geographical scope allows for an examination of potential cultural differences in cyber-security perceptions and biases. Additionally, the research updates the theoretical framework to account for recent developments in the cyber-threat landscape, acknowledging the impact of emerging technologies and increased cybercrime. This temporal contextualization ensures that the theoretical contributions are relevant to the current and evolving cyber-security environment.
3. **Focus on Cyber-Security Experts:** The shift in focus from general IT management to specialized cyber-security experts represents another key theoretical advancement. Engaging directly with cyber-security professionals rather than MIS executives, this research provides a more nuanced understanding of cyber-security behaviors and risk perceptions among those with deep expertise in the field. The findings reveal that even subject matter experts are susceptible to judgmental flaws, challenging the assumption that expertise equates to immunity from cognitive biases. This emphasis on expert perspectives enriches the theoretical framework, offering a more accurate and sophisticated depiction of how cognitive biases influence decision-making in the field.
4. **Integration of Organizational Practices:** The study also contributes theoretically by examining the intersection of cognitive biases and organizational practices. It reveals how biases interact with aspects such as reporting structures, audit practices, and crisis communication plans. While well-intentioned, this research indicates that using these practices in isolation—without a broader framework for addressing cognitive biases—may lead to unintended consequences and a false sense of preparedness. With 47% of participants confirming that the CISO reports to a Technology leader, such as the CIO or CTO, it infers that cyber-security might still often be viewed as an IT issue rather than a strategic priority. Notably, a trend emerged suggesting that CISOs reporting to non-Technology leaders may exhibit lower *overconfidence* due to the necessity of more rigorous communication and justification of cyber-security strategies. This finding, approaching statistical significance, points to the potential impact of reporting structures

on decision-making and highlights the need for further research into how organizational hierarchies influence cyber-security leadership and effectiveness.

5. **Advancement of Decision-Making Theories:** Strategic decision-making involves navigating uncertainty and ambiguity, with decision-makers often constrained by bounded rationality due to limited information and cognitive biases. These decisions, frequently made under time pressure and emotional weight, carry significant consequences for the organization. Effectively managing this uncertainty is crucial for enhancing cyber-resilience and successfully navigating the complex landscape of cyber-threats. Building on the theoretical foundations laid by Das and Teng (1999), Schwenk (1984), Tversky and Kahneman (1974), Weinstein (1980), and others regarding cognitive biases, this research applies these principles to the domain of cyber-security. While acknowledging the broader literature on decision-making under uncertainty, this study focuses on how these biases manifest in the context of cyber-security, thereby extending existing theories to address this emerging and increasingly relevant area.
6. **Addressing Research Gaps and Future Directions:** The research addresses several identified gaps in the literature, particularly the need for a comprehensive examination of biases in cyber-security decision-making. By broadening the scope of biases studied and updating the theoretical framework, the study sets the stage for future research to explore these dynamics in greater detail. A key theme is the need to better understand and address cognitive biases affecting cyber-security decision-making at all organizational levels. Attention should be paid to how cognitive biases are exhibited by IT and cyber practitioners compared to general users, as understanding these differences can inform more tailored training and decision-support systems. Further research should also delve into the evolving role of CISOs, examining how reporting structures and communication methods impact overall cyber-resilience. Evaluating structured decision-making frameworks, stress management, and succession planning for CISOs is also crucial for reducing biases and improving cyber-security practices. Given the rapidly changing cyber-threat landscape, it is important to explore how organizations can balance the benefits of external audits with the risks of overconfidence. Research should also aim to create metrics that accurately reflect an organization’s cyber-security status, ensuring resources are allocated based on actual needs. Lastly, the cultural dimensions of cyber-security, including varying risk perceptions across regions, require more exploration to tailor strategies effectively. Ultimately, advancing our

understanding of how cognitive biases and organizational structures interact will be crucial for improving cyber-security effectiveness and resilience.

In summary, this research makes significant theoretical contributions by extending cognitive bias frameworks, contextualizing findings geographically and temporally, emphasizing expert perspectives, integrating organizational practices, and advancing decision-making theories. These contributions provide a deeper and more nuanced understanding of cyber-security risk perceptions and behaviors, offering valuable insights for both researchers and practitioners in the field.

Practical Contributions and Recommendations

An important emphasis lies in reducing cognitive biases like *optimism bias*, *overconfidence*, and the *availability heuristic*, which have the potential to hinder efficient decision-making within the realm of cyber-security. By tackling these biases head-on, organizations can bolster their resilience against cyber-attacks and be better equipped to handle potential cyber-threats. The following top 10 suggestions are grounded in this research and offer practical, impactful measures for organizations to strengthen their cyber-security practices.

1. **Education and Training:** Regular training sessions for board members and cyber-professionals are crucial. This should include fostering critical thinking and reducing reliance on mental shortcuts, such as *optimism bias*, *overconfidence bias* or the presence of an *availability heuristic,* which can lead to inadequate preparedness. By incorporating workshops on cognitive biases and decision-making, organizations can enhance their ability to make informed and balanced decisions in the face of cyber-threats.
2. **Dedicated Cyber-Security Committees:** Establishing specialized cyber-security committees is crucial for enhancing cyber-resilience. The analysis indicates a positive correlation between frequent audits and *overconfidence bias*, suggesting that organizations with formal audit practices might exhibit inflated confidence in their cyber-security measures. To mitigate this risk, ensure that these committees not only supervise strategy formulation and execution but also critically evaluate and challenge the outcomes of audit reports and preparedness exercises. This will help counteract any *overconfidence* and ensure a more balanced and realistic approach to cyber-security.

3. **Facilitating Decision-Making Processes:** Developing clear and structured protocols to support strategic decision-making is essential. This includes defining precise steps, criteria, and evaluation methods to ensure decisions are based on thorough analysis rather than intuition or subjective opinions. Utilizing a data-driven approach, simulations, and modeling is crucial for providing unbiased insights to inform strategic decision-making, leading to well-informed and effective decisions based on accurate information. It is also recommended to regularly review these decision-making processes to incorporate lessons learned and adjust protocols based on evolving cyber-threat landscapes.
4. **Increased CISO Empowerment:** Cyber-risks pose a substantial threat to organizations, with the likelihood of this risk increasing further going forward. The analysis indicates that the effectiveness of cyber-security measures might be impacted by organizational practices related to audits and simulations. Strengthening the CISO's role can help address biases and enhance overall cyber-security. Given the findings that formal audits can sometimes increase overconfidence, it is important to empower CISOs to advocate for a holistic view of cyber-security that goes beyond audit results, ensuring comprehensive and adaptive security strategies. It is also crucial to empower CISOs by granting them the necessary authority and resources to enforce robust cyber-security protocols, while also ensuring that their recommendations are taken seriously and integrated into the broader business strategy.
5. **Regular Cyber-Security Briefings:** Scheduling regular briefings between the CISO and board members is crucial for keeping them up to date on current threats, weaknesses, and the overall cyber-security posture of the organization. Regular updates provide up-to-date information on existing risks, vulnerabilities, and cyber-security incidents, highlighting the dynamic and ongoing nature of cyber-threats. To counteract the potential overconfidence identified in the study, these briefings should also include critical reviews of past decisions and potential blind spots in current strategies. The observed trend linking infrequent fire drills to overconfidence highlights the need for ongoing updates to counteract any underestimation of risks.
6. **Removing Communication and Organizational Barriers:** The reporting structure of a CISO can influence *overconfidence bias*, affecting decision-making and risk evaluations. CISOs reporting to non-technical executives may need to adopt more System-2 thinking to effectively communicate complex cyber-security issues. The level of digital maturity within an organization, including its reliance on digital platforms for

revenue generation, should be closely linked to the proximity and access of the CISO function to the board. Integrating the CISO role directly into the board in digitally advanced organizations can address communication barriers and improve understanding. Conversely, positioning the role in middle management diminishes its importance. In the case of a cyber-security incident, inadequate access and airtime for the CISO may result in legal challenges related to the board's fiduciary duties. Such failures may result in sanctions and lawsuits, highlighting the need for robust oversight in cyber-security matters.

7. **Cyber-Security Metrics, Reporting, and Investments:** To ensure alignment across the organization, it is crucial to establish precise metrics and reporting systems to monitor cyber-security performance. This involves consistently sharing these metrics with the board to emphasize both areas of improvement and potential risks. Given the observed relationship between formal audits and overconfidence, it is recommended that these metrics include performance indicators from simulations, stress tests, and other dynamic assessments, beyond traditional audit results. It is advisable to determine cyber-security funding by referencing industry benchmarks, such as a percentage of overall revenues, rather than relying on the previous year's budget. Consulting IT analyst firms and professional associations and sharing best practices with peer companies can prevent underinvestment. Continuous investments in cyber-security are important to proactively prevent incidents, rather than reacting to specific threats. Allocating part of the budget for contingencies and establishing feedback mechanisms for reporting near misses and minor incidents are also essential.
8. **Stress Management and Support Programs:** Establishing initiatives to address stress and prevent burnout and fatigue in the cyber-security workforce is essential for maintaining vigilance. This includes managing workloads, providing adequate resources such as staffing and investments, and offering health support to improve job satisfaction and overall effectiveness. The well-being of employees may significantly influence the outcomes of cyber-security efforts. By prioritizing stress management, organizations can potentially reduce the risks linked to cognitive biases.
9. **CISO Succession Management:** Given the criticality of the role and the widely acknowledged talent shortage of cyber professionals in the marketplace, it is crucial to establish and uphold a strong succession plan for the CISO role. This strategy ensures a smooth transition and readiness in the event of the current CISO's departure. Recognizing the potential impact of leadership transitions on organizational confidence

and risk perception, succession planning should include interim strategies to maintain continuity and avoid unnecessary risk exposure during leadership changes. If the position remains vacant for an extended period, it could needlessly heighten the organization's risk exposure and create a vacuum should a crisis arise.

10. **Operational Excellence and 3rd Party Validation:** It is essential to consistently evaluate and validate cyber-security practices using external experts, while being mindful of the potential for these assessments to create a false sense of security. The observed trend linking frequent audits to overconfidence highlights the importance of contextualizing audit results. While audits and external validations are crucial, they should be interpreted with caution and complemented by regular simulations and dynamic assessments to provide a comprehensive view of the organization's cyber-security posture. This balanced approach ensures that audits lead to genuine improvements rather than fostering complacency.

REFERENCES

451 Research. (2022). *As API Use Grows Over 200%, Security Concerns from Developers and Enterprise Users Loom.* Retrieved Oct 5, 2023 from https://www.prnewswire.co.uk/news-releases/as-api-use-grows-over-200-security-concerns-from-developers-and-enterprise-users-loom-809074571.html

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *Ieee Access*, *9*, 121916-121929.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., & Sleeper, M. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, *50*(3), 1-41.

ACSC. (2022). *Annual Cyber Threat Report. July 2021 - June 2022*. https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

Adam, S. (2021). *The State of Ransomware 2021*. Retrieved Nov 30, 2023 from https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/

Aiello, M., Thompson, S., Randria, M., Reventlow, C., Shaul, G., & Vaughan, A. (2022). *2022 Global Chief Information Security Officer (CISO) Survey*. Heidrick & Struggles. https://www.heidrick.com/en/insights/compensation-trends/2022-global-chief-information-security-officer-ciso-survey

Akamai. (2019). *State of the Internet Security Report: Retailers Most Common Credential Stuffing Attack Victim; Points to Dramatic Rise in API Traffic as Key Trend*. Retrieved Oct 5, 2023 from https://www.akamai.com/newsroom/press-release/state-of-the-internet-security-retail-attacks-and-api-traffic

Akyazi, U., Van Eeten, M. J. G., Ganan, H., Akyazi, U., Van Eeten, M., & Gañán, C. H. (2021). *Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum* Workshop on the Economics of Information Security, https://repository.tudelft.nl/islandora/object/uuid%3A01cb117a-339c-42e9-9691-8456a12e3947

Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *IET Information Security*, *16*(5), 324-345.

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Aldridge, J., & Décary-Hétu, D. (2014). Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2436643

Algarni, A., & Malaiya, Y. (2016). *A consolidated approach for estimation of data security breach costs* Proceedings of 2016 International Conference on Information Management (ICIM), May 7-8, London, United Kingdom.

Ali, S. E. A., Lai, F.-W., Hassan, R., & Shad, M. K. (2021). The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context of Efficient Market Hypothesis. *Sustainability*, *13*(3), 1066. https://www.mdpi.com/2071-1050/13/3/1066

Allen, T., Wells, E., & Klima, K. (2020). Culture and cognition: Understanding public perceptions of risk and (in)action. *IBM Journal of Research and Development*, *64*(1/2), 11:11-11:17. https://doi.org/10.1147/JRD.2019.2952330

Alnifie, K. M., & Kim, C. (2023). Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. *Journal of Information Security*, *14*(2), 93-110. https://doi.org/10.4236/JIS.2023.142007

Alqahtani, A., & Sheldon, F. T. (2022). A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. *Sensors 2022, Vol. 22, Page 1837*, *22*(5), 1837-1837. https://doi.org/10.3390/S22051837

Alrwais, S., Liao, X., Mi, X., Wang, P., Wang, X., Qian, F., Beyah, R., & McCoy, D. (2017). Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks. 2017 IEEE Symposium on Security and Privacy (SP), May 22-26, San Jose, CA, USA.

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A Systematic Review of multi-perspectives on human Cybersecurity Behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Ament, C. (2017). *The ubiquitous security expert: Overconfidence in information security* 38th ICIS 2017, Dec 10-13, Seoul, South Korea.

Ament, C., & Haag, S. (2016). *How information security requirements stress employees* 37th ICIS 2016 Proceedings, Dec 11-14, Dublin, Ireland. https://aisel.aisnet.org/icis2016/ISSecurity/Presentations/9/

Ament, C., & Jaeger, L. (2017). *Unconscious on their own ignorance: overconfidence in information security* Pacific Asia Conference on Information Systems (PACIS), Jul 16-20, Langkawi Island, Malaysia.

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177-1206. https://EconPapers.repec.org/RePEc:spr:reaccs:v:23:y:2018:i:3:d:10.1007_s11142-018-9452-4

Anderson, R. (2001). *Why Information Security is Hard-An Economic Perspective* Annual Computer Security Applications Conference (ACSAC), Dec 10-14, New Orleans, LA, USA.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., & Moore, T. (2018). Measuring the Changing Cost of Cybercrime. *The 18th Annual Workshop on the Economics of Information Security*. https://www.repository.cam.ac.uk/items/a9e1b7b4-03c6-43b5-ae0c-b5b59e0d4684

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. *The Economics of Information Security and Privacy*, 265-300. https://doi.org/10.1007/978-3-642-39498-0_12

Andrade, C. (2020). The limitations of online surveys. *Indian journal of psychological medicine*, *42*(6), 575-576.

Andrew, J., Victor, L., Jenny, C., Scott, J., LaFoy, & Sohn, E. (2015). *North Korea's Cyber Operations*. C. f. S. a. I. S. (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

Arghire, I. (2023). *EU Organizations Warned of Chinese APT Attacks*. Retrieved Jul 16, 2023 from https://www.securityweek.com/eu-organizations-warned-of-chinese-apt-attacks/

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1 - attackers. *IEEE Security and Privacy*, *13*(1), 71-76. https://doi.org/10.1109/MSP.2015.19

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). 2020 Cybercrime Economic Costs: No Measure No Solution. *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, 701-710. https://doi.org/10.1109/ARES.2015.56

Ashford, W. (2017). *Businesses blame rivals for DDoS attacks*. ComputerWeekly. Retrieved Jul 2, 2023 from https://www.computerweekly.com/news/450414239/Businesses-blame-rivals-for-DDoS-attacks

Ashraf, N., Camerer, C. F., & Loewenstein, G. (2005). Adam Smith, Behavioral Economist. *Journal of Economic Perspectives*, *19*(3), 131-145. https://doi.org/10.1257/089533005774357897

Atrews, R. A. (2020). Cyberwarfare: Threats, Security, Attacks, and Impact. *Journal of Information Warfare*, *19*(4). https://www.jinfowar.com/journal/volume-19-issue-4/cyberwarfare-threats-security-attacks-impact

Aufreiter, N., Huber, C., & Usher, O. (2022). *The role of the board in preparing for extraordinary risk*. McKinsey & Company. Retrieved Dec 11, 2023 from https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/the-role-of-the-board-in-preparing-for-extraordinary-risk

Avery, D. (2022). *Capital One $190 Million Data Breach Settlement: Today Is the Last Day to Claim Money*. CNET. Retrieved Oct 12, 2023 from https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/

Bahreini, F., Cavusoglu, A., Cenfetelli, H., & T., R. (2023). How "What you think you know about cybersecurity" can help users make more secure decisions. *Information & Management*, *60*(7), 103860. https://doi.org/10.1016/j.im.2023.103860

Bair, J., & Blas, J. (2021). *Petrol shortages sweep US as Colonial Pipeline remains down*. Aljazeera. Retrieved Jun 21, 2023 from https://www.aljazeera.com/economy/2021/5/11/petrol-shortages-sweep-us-as-colonial-pipeline-remains-down

Baldini, G., Barrero, J., & Chaudron, S. (2020). *Cybersecurity, our digital anchor – A European perspective*. European Commission, Joint Research Centre, Publications Office. https://doi.org/doi/10.2760/352218

Balebako, R., & Cranor, L. (2014). Improving App Privacy: Nudging App Developers to Protect User Privacy. *IEEE Security & Privacy*, *12*(4), 55-58. https://doi.org/10.1109/msp.2014.70

Bambysheva, N., & Linares, M. G. S. (2022). *Over $3 Billion Stolen In Crypto Heists: Here Are The Eight Biggest*. Forbes. Retrieved Nov 5, 2023 from https://www.forbes.com/sites/ninabambysheva/2022/12/28/over-3-billion-stolen-in-crypto-heists-here-are-the-eight-biggest/

Baraniuk, C. (2016). *Tor: 'Mystery' spike in hidden addresses*. BBC. Retrieved Aug 23, 2023 from https://www.bbc.com/news/technology-35614335

Barnes, L. R., Gruntfest, E. C., Hayden, M. H., Schultz, D. M., & Benight, C. (2007). False Alarms and Close Calls: A Conceptual Model of Warning Accuracy. *Weather and Forecasting*, *22*(5), 1140-1147. https://doi.org/10.1175/WAF1031.1

Baron, R. A. (2008). The role of affect in the entrepreneurial process. *The Academy of Management Review*, *33*(2), 328-340. https://doi.org/10.2307/20159400

Barrett, D. (2023). *Computer system used to hunt fugitives is still down 10 weeks after hack*. The Washington Post. Retrieved Aug 18, 2023 from https://www.washingtonpost.com/national-security/2023/05/01/marshals-hack-fugitives-surveillance-shutdown/

BBC. (2023). *Optus: Telecom boss Kelly Bayer Rosmarin quits after Australian outage*. Retrieved Dec 9, 2023 from https://www.bbc.com/news/world-australia-67470796

Becker, G. (1962). Irrational Behavior and Economic Theory. *Journal of Political Economy*, *70*, 1-13.

Becker, G. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, *76*(2), 169-217.

Becker, G. (1976). *The economic approach to human behavior* (Vol. 803). University of Chicago press.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51-61. https://doi.org/10.1016/j.chb.2015.01.039

Bennett, A., & Checkel, J. T. (2014). *Process Tracing: From Metaphor to Analytic Tool*. Cambridge University Press. https://doi.org/10.1017/CBO9781139858472

Bennett, S., & Maton, K. (2010). Beyond the ‘digital natives’ debate: Towards a more nuanced understanding of students' technology experiences. *Journal of Computer Assisted Learning*, *26*(5), 321-331. https://doi.org/10.1111/J.1365-2729.2010.00360.X

Bergh, C., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science*, *7*, 5. https://doi.org/10.1186/s40163-018-0079-3

Bernik, I. (2016). Cybercrime: The Cost of Investments into Protection. *Journal of Criminal Justice and Security*, *16*(2), 105-116.

Bhatt, S., & Shiva, A. (2020). Empirical examination of the adoption of Zoom software during COVID-19 pandemic: Zoom TAM. *Journal of Content, Community and Communication*, *12*(6), 70-88.

Bing, C., & Satter, R. (2023). *Hacktivists stoke Israel-Gaza conflict online*. Reuters. Retrieved Dec 7, 2023 from https://www.reuters.com/world/middle-east/hacktivists-stoke-israel-gaza-conflict-online-2023-10-11/

BKA. (n. d.). *What is cybercrime?* Retrieved Jun 23, 2023 from https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html

Blackborow, J., & Christakis, S. (2019). *Complexity In Cybersecurity Report 2019*.

Blackwill, R. D., & Gordon, P. H. (2018). *Containing Russia - How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge.* . https://cdn.cfr.org/sites/default/files/report_pdf/CSR80_BlackwillGordon_ContainingRussia.pdf

Böhme, R. (2005). Cyber-Insurance Revisited. Workshop on the Economics of Information Security,

Böhme, R., & Kataria, G. (2006). On the limits of cyber-insurance. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *4083 LNCS*, 31-40. https://doi.org/10.1007/11824633_4/COVER

Böhme, R., Laube, S., & Riek, M. (2020). A Fundamental Approach to Cyber Risk Analysis. *Variance*, *12*(2), 161-185.

Bone, J. (2016). Cognitive Risk Framework for Cybersecurity: Bounded Rationality. *EDPACS*, *54*(5), 1-11. https://doi.org/10.1080/07366981.2016.1247564

Bone, J. (2021). Cognitive Risks. *EDPACS*, *64*(1), 1-8. https://doi.org/10.1080/07366981.2020.1840020

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342-353. https://doi.org/10.1016/J.TECHNOVATION.2014.02.001

Brady, H., & Collier, D. (2010). *Rethinking Social Inquiry: Diverse Tools, Shared Standards* (2nd ed.). Rowman & Littlefield Publishers.

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, *2018*. https://doi.org/10.1155/2018/1798659

Brattberg, E., & Maurer, T. (2018). *Five European Experiences With Russian Election Interference*. C. E. f. I. Peace. http://www.jstor.org/stable/resrep21009.6

Brenner, S. W. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, *97*(2).

https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=7260&context=jclc

Bringsjord, S., & Licato, J. (2015). By Disanalogy, Cyberwarfare Is Utterly New. *Philosophy and Technology*, *28*(3), 339-358. https://doi.org/10.1007/S13347-015-0194-Y

British Transport Police. (n. d.). *The Great Train Robbery, 1963*. British Transport Police. Retrieved Nov 8, 2023 from https://www.btp.police.uk/police-forces/british-transport-police/areas/about-us/about-us/our-history/crime-history/great-train-robbery/

Brooks, B., Curnin, S., Owen, C., & Bearman, C. (2020). Managing cognitive biases during disaster response: the development of an aide memoire. *Cognition, Technology & Work*, *22*. https://doi.org/10.1007/s10111-019-00564-5

Bruijne, M. d., Eeten, M. v., Gañán, C. H., & Pieters, W. (2017). *Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment*. https://repository.wodc.nl/bitstream/handle/20.500.12832/2299/2740_Summary_tcm28-273244.pdf?sequence=2&isAllowed=y

Buckland, B. S., Schreier, F., & Winkler, T. H. (2015). *Democratic Governance Challenges of Cyber Security*. DCAF Horizon. https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(S1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973

Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming, 2nd ed*. Routledge/Taylor & Francis Group.

Caesar, E. (2020). *The Cold War Bunker That Became Home to a Dark-Web Empire*. New Yorker. Retrieved Aug 27, 2023 from https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire

Cambridge Centre for Risk Studies, & Lloyd's of London. (2015). *Business Blackout. The insurance implications of a cyber-attack on the US power grid*. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf

Cameron, D. (2017). *Ransomware Markets Are Exploding, Study Finds*. Gizmodo. Retrieved Aug 14, 2023 from https://gizmodo.com/ransomware-markets-are-exploding-study-finds-1819855646

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, *11*, 431-448. https://doi.org/10.3233/JCS-2003-11308

Canadian Centre for Cyber Security. (n. d.). *An introduction to the cyber threat environment*. Retrieved Jun 26, 2023 from https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Candrick, W., Addiscott, R., Walls, A., & Michaels, A. (2023). *Security Awareness Efforts Fall Short! Now What? (Survey Results Analysis)*. Gartner.

Carr, N. G. (2003). IT Doesn't Matter. *Harvard Business Review*, *81*, 41-49.

Cary, D. (2021). *China's National Cybersecurity Center* (Center for Security and Emerging Technology (CSET), Issue. https://doi.org/10.51593/2020CA016

Castells, M. (2010). *End of Millennium: With a New Preface, Volume III, Second Edition With a New Preface*. Wiley-Blackwell. https://doi.org/10.1002/9781444323436

Central Statistics Office. (2020). *Crime and Victimisation 2019 - CSO - Central Statistics Office*. Retrieved Jul 12, 2023 from https://www.cso.ie/en/releasesandpublications/ep/p-cv/crimeandvictimisation2019/

Ceric, A., & Holland, P. (2019). The role of cognitive biases in anticipating and responding to cyberattacks. *Information Technology and People*, *32*(1), 171-188. https://doi.org/10.1108/ITP-11-2017-0390/FULL/XML

CFR. (2022). Retrieved Jul 8, 2023 from https://www.cfr.org/cyber-operations/targeting-organizations-asia-europe-and-north-america

CFR. (n. d.-a). Retrieved Jul 8, 2023 from https://www.cfr.org/cyber-operations/muddywater

CFR. (n. d.-b). *APT 10*. Retrieved Jul 5, 2023 from https://www.cfr.org/cyber-operations/apt-10

CFR. (n. d.-c). *Equation Group*. Retrieved Jul 1, 2023 from https://www.cfr.org/cyber-operations/equation-group

CFR. (n. d.-d). *North Korea's Military Capabilities*. Retrieved Jul 3, 2023 from https://www.cfr.org/backgrounder/north-korea-nuclear-weapons-missile-tests-military-capabilities

Chander, A., Kaminski, M. E., & McGeveran, W. (2020). Catalyzing privacy law. *Minn. L. Rev.*, *105*(4), 1733-1802. https://doi.org/https://dx.doi.org/10.2139/ssrn.3433922

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, *38*, 100467-100467. https://doi.org/10.1016/J.ACCINF.2020.100467

Chanlett-Avery, E., Rosen, L. W., & et al. (2017). *North Korean Cyber Capabilities: In Brief*. https://sgp.fas.org/crs/row/R44912.pdf

Chen, J. Q., & Dinerman, A. (2018). Cyber capabilities in modern warfare. *Intelligent Systems, Control and Automation: Science and Engineering*, *93*, 21-30. https://doi.org/10.1007/978-3-319-75307-2_2

Chen, T., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, *44*(4), 91-93.

Chickowski, E. (2019, Oct 1). Every Hour SOCs Run, 15 Minutes Are Wasted on False Positives. https://www.bitdefender.com/blog/businessinsights/every-hour-socs-run-15-minutes-are-wasted-on-false-positives/

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11.

Choi, K.-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2*(1).

Cimpanu, C. (2017). *Man Uses DDoS-for-Hire Services to Attack Former Employer, Taunts Firm via Email*. BleepingComputer.com. Retrieved Jul 8, 2023 from https://www.bleepingcomputer.com/news/security/man-uses-ddos-for-hire-services-to-attack-former-employer-taunts-firm-via-email

Cimpanu, C. (2019). *'Carpet-bombing' DDoS attack takes down South African ISP for an entire day*. ZDNet. Retrieved Dec 5, 2023 from https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

CISA. (2020). Retrieved Jul 5, 2023 from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a

CISA. (2021a). Retrieved Jul 2, 2023 from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

CISA. (2021b). *Cyber-Attack Against Ukrainian Critical Infrastructure*. Retrieved Aug 5, 2023 from https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA. (2021c). *Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities*. Retrieved Aug 20, 2023 from https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a

CISA. (2022a). *2021 Trends Show Increased Globalized Threat of Ransomware*. Retrieved Jun 30, 2023 from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a

CISA. (2022b). *Protecting Against Cyber Threats to Managed Service Providers and their Customers*. Retrieved Jun 30, 2023 from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a

CISA. (2023). *Review Of The Attacks Associated with Lapsus$ And Related Threat Groups Executive Summary*. https://www.cisa.gov/resources-tools/resources/review-attacks-associated-lapsus-and-related-threat-groups-executive-summary

CISA. (n. d.-a). Retrieved Jul 5, 2023 from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a

CISA. (n. d.-b). *North Korea Cyber Threat Overview and Advisories*. Retrieved Jul 8, 2023 from https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea

CISA. (n. d.-c). *Russia Cyber Threat Overview and Advisories*. Retrieved Jun 26, 2023 from https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia

Cisco. (2023). *2023 Global Networking Trends Report*. https://www.cisco.com/c/en_uk/solutions/enterprise-networks/xa-09-2023-networking-report.html

Clemons, E. K., & Weber, B. W. (1990). Strategic Information Technology Investments: Guidelines for Decision Making. *Journal of Management Information Systems*, *7*(2), 9-28. https://doi.org/10.1080/07421222.1990.11517887

Cliff, G., & Desilets, C. (2014). White collar crime: What it is and where it's going. *Notre Dame Journal of Law, Ethics & Public Policy*, *28*, 481-523.

Cohen, G. (2021). *Throwback Attack: How the modest Bowman Avenue Dam became the target of Iranian hackers*. Retrieved Aug 27, 2023 from https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*. https://doi.org/10.2307/2094589

Collins, M., et al. (2016). *Common Sense Guide to Mitigating Insider Threats*. Carnegie Mellon University. Software Engineering Institute.

Cook, S., Giommoni, L., Pareja, N. T., Levi, M., Williams, M. L., & Pareja, N. T. (2023). Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory. *The British Journal of Criminology*, *63*(2), 384-406. https://doi.org/10.1093/BJC/AZAC021

Copeland, T. (2020). *Binance CEO blames rival exchanges for DDoS attacks*. Retrieved Jul 6, 2023 from https://decrypt.co/27016/binance-ceo-blames-rival-exchanges-over-ddos-attacks

Cordey, S. (2023). *Software Supply Chain Attacks: An Illustrated Typological Review* (CSS Cyberdefense Reports, Issue. E. Zurich. https://doi.org/10.3929/ethz-b-000584947

Corera, G. (2023). *Russia hacking: 'FSB in years-long cyber attacks on UK', says government*. BBC. Retrieved Dec 7, 2023 from https://www.bbc.com/news/uk-politics-67647548

Cossin, D., & Lu, A. (2021). *Board Oversight of Cyber Risks and Cybersecurity*. https://www.imd.org/research-knowledge/corporate-governance/articles/board-oversight-cyber-risks-cybersecurity/

Coveware. (2021). *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound*. Retrieved Nov 30, 2023 from https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

Craig, A., & Valeriano, B. (2016). Conceptualising cyber arms races. 2016 8th International Conference on Cyber Conflict (CyCon), May 31-Jun 3, Tallinn, Estonia.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432-448. https://doi.org/10.1016/j.jfineco.2022.12.002

Crowdstrike. (n. d.). Retrieved Jun 25, 2023 from https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Engineering Management Review*, *47*, 79-86. https://doi.org/10.1109/EMR.2019.2927559

Cyentia Institute. (2019). *Cloud Risk Surface Report*.

D'Hoinne, J., Watts, J., Olyaei, S., & Witty, R. (2022). *Prepare for New and Unpredictable Cyberthreats*. Gartner. https://www.gartner.com/document/4015489

D'Hoinne, J., Watts, J., & Thielemann, K. (2022). *How to Respond to the 2022 Cyberthreat Landscape*. Gartner. https://www.gartner.com/document/4013107

Dal Cin, P., Abend, V., Barton, R., & Seedat, Y. (2023). *The Cyber-Resilient CEO*.

Das, S., & Nayak, T. (2013). Impact of Cyber Crime: Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(2), 142-153.

Das, T. K., & Teng, B. S. (1999). Cognitive Biases and Strategic Decision Processes: An Integrative Perspective. *Journal of Management Studies*, *36*(6), 757-778. https://doi.org/10.1111/1467-6486.00157

Dash, G., & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, *173*, 121092. https://doi.org/10.1016/j.techfore.2021.121092

DataDome. (2020). Retrieved Jul 3, 2023 from https://datadome.co/threats/when-competition-gets-dirty-surviving-a-layer-7-ddos-attack

Davidson, J., Aiken, M., & Phillips, K. (2022). *European Youth Cybercrime, Online Harm and Online Risk Taking: 2022 Research Report*. https://uel.ac.uk/about-uel/news/2022/december/two-thirds-european-youth-involved-some-form-cybercrime-online-risk-taking

Davies, C., & Chipolina, S. (2022). *How North Korea became a mastermind of crypto cyber crime*. Financial Times. Retrieved Jul 2, 2023 from https://www.ft.com/content/dec696d4-fd51-4cce-bbd9-1dee911eb4cd

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), 1796-1808. https://doi.org/10.1080/0144929X.2021.1905066

de Neira, A. B., Kantarci, B., & Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks*, *222*, 109553.

Dean Jr., J. W., & Sharfman, M. P. (1993). Procedural Rationality In The Strategic Decision-Making Process. *Journal of Management Studies*, *30*(4), 587-610. https://doi.org/10.1111/j.1467-6486.1993.tb00317.x

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55-75. https://doi.org/10.1007/S10611-016-9644-4

Delamarter, A. (2016). *The Darknet: A Quick Introduction for Business Leaders*. Harvard Business Review. Retrieved Oct 5, 2023 from https://hbr.org/2016/12/the-darknet-a-quick-introduction-for-business-leaders

Deloitte. (2022). *Cyber Trends an Intelligence Report 2022*. https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/risk/cr/jp-cr-deloitte-cyber-trends-and-intelligence-report-2022-e.pdf

Demirdjian, Z., & Mokatsian, Z. (2015). The Costs of Cybercrimes to Business and Society. *American Society of Business and Behavioral Sciences*, *22*(1), 104-109.

Denić, N. V., & Devetak, S. (2023). Dark Web – As Challenge of the Contemporary Information Age. *TRAMES*, *XXVII*(2), 115-126.

DeNisco Rayome, A. (2017). *Why ex-employees may be your company's biggest cyberthreat*. Tech Republic. Retrieved Jul 4, 2023 from https://www.techrepublic.com/article/why-ex-employees-may-be-your-companys-biggest-cyberthreat

Denning, D. E. (2000). *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, Committee on Armed Services on May 23, 2000*. https://irp.fas.org/congress/2000_hr/00-05-23denning.htm

Dennis, N., Erdos, G., & Robinson, D. (2003). *The Failure of Britain's Police*. The Cromwell Press.

Dhingra, N., Gorn, Z., Kener, A., & Dana, J. (2012). The default pull: An experimental demonstration of subtle default effects on preferences. *Judgment and Decision Making*, *7*(1), 69-76. https://doi.org/10.1017/S1930297500001844

Dictionary of Military and Associated Terms. (2005). Retrieved Jul 5, 2023 from https://www.thefreedictionary.com/strategic+vulnerability

Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. *Risk Management and Insurance Review*, *23*(2), 183-208. https://doi.org/10.1111/RMIR.12151

Dillon, R., & Tinsley, C. (2016). Near-miss events, risk messages, and decision making. *Environment Systems and Decisions*, *36*. https://doi.org/10.1007/s10669-015-9578-x

Dimara, E., Franconeri, S., Plaisant, C., Bezerianos, A., & Dragicevic, P. (2018). A task-based taxonomy of cognitive biases for information visualization. *IEEE transactions on visualization and computer graphics*, *26*(2), 1413-1432.

Dong, K., Lin, R., Yin, X., & Xie, Z. (2021). How does overconfidence affect information security investment and information security performance? *Enterprise Information Systems*, *15*(4), 474-491.

Druckman, J. N., & McDermott, R. (2008). Emotion and the Framing of Risky Choice. *Political Behavior*, *30*(3), 297-321. http://www.jstor.org.wwwproxy1.library.unsw.edu.au/stable/40213319

Duong, A. A., Maurushat, A., & Bello, A. (2022). Working from home users at risk of COVID-19 ransomware attacks. *Cybersecurity and Cognitive Science*, 51-87. https://doi.org/10.1016/B978-0-323-90570-1.00001-2

ECB. (2022). *IT and cyber risk – key observations - ECB Banking Supervision*. https://www.bankingsupervision.europa.eu/banking/srep/2022/html/ssm.srep2022_ITandcyberrisk.en.pdf

EDA. (n. d.). Retrieved Jul 17, 2023 from https://eda.europa.eu/what-we-do/all-activities/activities-search/hybrid-warfare

Egloff, F. J., & Smeets, M. (2023). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, *46*(3), 502-533. https://doi.org/10.1080/01402390.2021.1895117

Ehrlich, I. (1996). Crime, Punishment, and the Market for Offenses. *Journal of Economic Perspectives*, *10*(1), 43-67. https://doi.org/10.1257/JEP.10.1.43

Eisenhardt, K. M., & Zbaracki, M. (1992). Strategic decision making. *Strategic Management Journal*, *13*, 17-37.

Eling, M., & Jung, K. (2024). Optimism bias and its impact on cyber risk management decisions. *Risk Sciences*, *1*, 100001. https://doi.org/10.1016/j.risk.2024.100001

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474-491. https://doi.org/10.1108/JRF-09-2016-0122

Eling, M., & Wirfs, J. H. (2016). *Cyber risk: too big to insure? Risk transfer options for a mercurial risk class*. University of St. Gallen.

EMCRC. (2022). *"Script Kiddies" as young as nine conduct DDoS attacks*. East Midlands Cyber Resilience Centre. Retrieved Jul 9, 2023 from https://www.emcrc.co.uk/post/script-kiddies-as-young-as-nine-conduct-ddos-attacks

Emery, N. E. (2005). The Myth of Cyberterrorism. *Journal of Information Warfare*, *4*(1), 80-89.

ENISA. (2021). *Threat Landscape for Supply Chain Attacks*.

ENISA. (2022a). *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

ENISA. (2022b). *Threat Landscape*. Retrieved Jul 1, 2023 from https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

ENISA. (2023). *JP-23-01 - Sustained activity by specific threat actors*. https://cert.europa.eu/files/data/TLP-CLEAR-JointPublication-23-01.pdf

Eoyang, M., & et al. (2018). *To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors – Third Way*. https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors

Eppler, M., & Muntwiler, C. (2021). BIASMAP–developing a visual typology and interface to explore and understand decision-making errors in management. Human Interaction, Emerging Technologies and Future Applications IV: Proceedings of the 4th International Conference on Human Interaction and Emerging Technologies: Future Applications (IHIET–AI 2021), Apr 28-30, Strasbourg, France.

Esfandiari, G. (2020). *Iran To Work With China To Create National Internet System*. Retrieved Jul 8, 2023 from https://www.rferl.org/a/iran-china-national-internet-system-censorship/30820857.html

European Commission. (2020). *Europeans' attitudes towards cyber security (cybercrime)*. https://europa.eu/eurobarometer/surveys/detail/2249

Europol. (2021). *DarkMarket: world's largest illegal dark web marketplace taken down*. Retrieved Jun 23, 2023 from https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

Europol. (2022). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021#downloads.

Europol. (2023a). *288 dark web vendors arrested in major marketplace seizure*. Retrieved Aug 14, 2023 from https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

Europol. (2023b). *Cyber-attacks: the apex of crime-as-a-service (IOCTA 2023)*. https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023#downloads

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research*, *15*(2), 195-219.

Evans, J. R., & Mathur, A. (2018). The value of online surveys: a look back and a look ahead. *Internet Research*, *28*(4), 854-887. https://doi.org/10.1108/IntR-03-2018-0089

EY. (2021). *Global Information Security Survey 2021*.

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity Indices and Cybercrime Annual Loss and Economic Impacts. *Journal of Business and Behavioral Sciences*, *32*(1), 63-71.

Farahmand, F. (2018). *Applying Behavior Economics to Improve Cyber Security Behaviors* (AD1057994). G. I. o. Technology. https://apps.dtic.mil/sti/citations/AD1057994

Fatoki, J. G., Shen, Z., & Mora-Monge, C. A. (2024). Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior. *Computers & Security*, *141*, 103812. https://doi.org/10.1016/j.cose.2024.103812

FBI. (2016). *Russian Interference in 2016 U.S. Elections*. Retrieved Aug 12, 2023 from https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

FBI. (2020). Retrieved Jul 5, 2023 from https://www.ic3.gov/Media/News/2020/201030.pdf

FBI. (2021). *Internet Crime Report*. https://www.ic3.gov/media/PDF/AnnualReport/2021_IC3Report.pdf

FBI. (2023). *FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft*. Retrieved Jul 12, 2023 from https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft

FE Digital Currency. (2023). *Hydra Market clocked highest revenue among darknet markets for 2022*. Retrieved Jul 15, 2023 from https://www.financialexpress.com/business/blockchain-hydra-market-clocked-highest-revenue-among-darknet-markets-for-2022-blog-2989425

Felson, M., & Boivin, R. (2015). Daily crime flows within a city. *Crime Science*, *4*(1), 1-10. https://doi.org/10.1186/S40163-015-0039-0/TABLES/9

Ferretti, V., Guney, S., Montibeller, G., & Winterfeldt, D. V. (2016). Testing Best Practices to Reduce the Overconfidence Bias in Multi-criteria Decision Analysis. 49th Hawaii International Conference on System Sciences (HICSS), Jan 5-8, Koloa, HI, USA.

Fielder, A., König, S., Panaousis, E., Schauer, S., & Rass, S. (2018). Risk Assessment Uncertainties in Cybersecurity Investments. *Games*, *9*. https://doi.org/10.3390/g9020034

Finkle, J., & Quadir, S. (2016). *Exclusive: SWIFT to advise banks on security as Bangladesh hack details emerge*. Reuters. Retrieved Dec 6, 2023 from https://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0WM0ZS/

Florêncio, D., & Herley, C. (2011). Sex, Lies and Cyber-crime Survey. *Workshop on the Economics of Information Security*.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *The Review of Financial Studies*, *32*(5), 1798-1853. https://doi.org/10.1093/rfs/hhz015

Forscey, D., Bateman, J., Beecroft, N., & Woods, B. (2022). *Systemic Cyber Risk: A Primer*. https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531

France24. (2020). *French hospital suspends operations after cyber attacks*. Retrieved Aug 21, 2023 from https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks

Frank, M. (2020). *Using calibration to help overcome information security overconfidence* Dec 13-16, ICIS 2020, Hyderabad, India.

Franke, U. (2020). IT service outage cost: case study and implications for cyber insurance. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *45*(4), 760-784.

Fraunhofer. (n. d.-a). *APT10*. Retrieved Jul 1, 2023 from https://malpedia.caad.fkie.fraunhofer.de/actor/apt10

Fraunhofer. (n. d.-b). *Equation Group*. Retrieved Jul 1, 2023 from https://malpedia.caad.fkie.fraunhofer.de/actor/equation_group

Fraunhofer. (n. d.-c). *MuddyWater*. Retrieved Jul 2, 2023 from https://malpedia.caad.fkie.fraunhofer.de/actor/muddywater

Freeman, R. (1999). The economics of crime. *3, Part C*, 3529-3571. https://EconPapers.repec.org/RePEc:eee:labchp:3-52

Fricker, R. D., & Schonlau, M. (2002). Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature. *Field Methods*, *14*, 347 - 367.

Gable, K. (2010). Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Journal of Transnational Law*, *43*(1). https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1343&context=vjtl

Gächter, S., Johnson, E. J., & Herrmann, A. (2022). Individual-level loss aversion in riskless and risky choices. *Theory and Decision*, *92*(3), 599-624. https://doi.org/10.1007/s11238-021-09839-8

Gainsbury, S. M., Browne, M., & Rockloff, M. (2019). Identifying risky Internet use: Associating negative online experience with specific online behaviours. *New Media & Society*, *21*(6), 1232-1252. https://doi.org/10.1177/1461444818815442

Galeotti, M. (2017). *Crimintern: How the Kremlin uses Russia's criminal networks in Europe*. https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/

Garg, P. (2019). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, *49*(2), 503-519.

Garg, V., & Camp, L. (2011). Heuristics and Biases: Implications for Security Design. *Information Technology & Systems eJournal*, *32*. https://doi.org/10.1109/MTS.2013.2241294

Gartner. (2020). *Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations*. Retrieved Dec 26, 2023 from https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w

Gartner. (2022). *What Is Cybersecurity?* Retrieved Dec 2, 2023 from https://www.gartner.com/en/topics/cybersecurity

Gartner. (2023). *Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024*. Retrieved Dec 26, 2023 from https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

Gaspareniene, L., Remeikiene, R., & Navickas, V. (2016). The Concept of Digital Shadow Economy: Consumer's Attitude. *Procedia Economics and Finance*, *39*, 502-509. https://doi.org/10.1016/S2212-5671(16)30292-1

Gaspareniene, L., Remeikiene, R., & Schneider, F. G. (2018). The definition of digital shadow economy. *Technological and Economic Development of Economy*, *24*(2), 696-717. https://doi.org/10.3846/20294913.2016.1266530

Gatlan, S. (2019). *Global Shipping Firm Pitney Bowes Affected by Ransomware Attack*. BleepingComputer.com. Retrieved Jul 12, 2023 from https://www.bleepingcomputer.com/news/security/global-shipping-firm-pitney-bowes-affected-by-ransomware-attack/

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

Giannangeli, M. (2008). *Are we ready for Russian Mafia's crime revolution*. Sunday Express.

Gibbs, S., Moore, K., Steel, G., & McKinnon, A. (2017). The Dunning-Kruger Effect in a workplace computing setting. *Computers in Human Behavior*, *72*. https://doi.org/10.1016/j.chb.2016.12.084

Gigerenzer, G. (2015). On the Supposed Evidence for Libertarian Paternalism. *Review of Philosophy and Psychology*, *6*(3), 361-383. https://doi.org/10.1007/s13164-015-0248-1

Gleason, M. (2023). *Microsoft Loop crosses information silos in 365*. TechTarget. Retrieved Oct 6, 2023 from https://www.techtarget.com/searchunifiedcommunications/feature/Microsoft-Loop-crosses-information-silos-in-365

Glenny, M. (2023). *The untold history of today's Russian-speaking hackers*. Financial Times. Retrieved Aug 15, 2023 from https://www-ft-com.ezp.lib.cam.ac.uk/content/9ac188be-8bcf-4b5a-8051-10563683b979

Goel, S. (2020). How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections*, *19*(1), 87-95. https://www.jstor.org/stable/26934538

Goel, V. (2017). *One Billion Yahoo Accounts Still for Sale, Despite Hacking Indictments*. New York Times. Retrieved Aug 2, 2023 from https://www.nytimes.com/2017/03/17/technology/yahoo-hack-data-indictments.html

Golden, R. S., S. (2017). *Why do former employees still have access to company networks?* https://www.hrdive.com/news/why-do-former-employees-still-have-access-to-company-networks/447322

Gomez, M. A., & Villar, E. B. (2018). Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance*, *6*(2), 61-72.

Goodell, J. W., & Corbet, S. (2023). Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. *Finance Research Letters*, *51*, 103329-103329. https://doi.org/10.1016/J.FRL.2022.103329

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223. https://doi.org/10.1093/IJLIT/10.2.139

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, *06*(01), 24-30. https://doi.org/10.4236/JIS.2015.61003

Gramenz, J. (2020). *Teen charged over alleged DDoS hack that took school district offline*. Retrieved Jul 7, 2023 from https://www.news.com.au/technology/online/hacking/teen-charged-over-alleged-ddos-hack-that-took-school-district-offline/news-story/176df651e74db5e5c8e5d6dc1ad55436

Gramer, R., & Iyengar, R. (2023). *How North Korea's Hackers Bankroll Its Quest for the Bomb*. Retrieved Jul 8, 2023 from https://foreignpolicy.com/2023/04/17/north-korea-nuclear-cyber-crime-hackers-weapons

Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Weird. Retrieved Dec 4, 2023 from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gunawan, B., Ratmono, B., & Abdullah, A. (2023). Cybersecurity and Strategic Management. *Foresight and STI Governance*, *17*, 88-97. https://doi.org/10.17323/2500-2597.2023.3.88.97

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7). https://doi.org/10.1016/j.heliyon.2017.e00346

Hajizada, A., & Moore, T. (2023). On Gaps in Enterprise Cyber Attack Reporting. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Jul 3-7, Delft, Netherlands.

Haley, U., & Stumpf, S. A. (1989). Cognitive trails in strategic decision-making: linking theories of personalities and cognitions. *Journal of Management Studies*, *26*(5), 477-497.

Hancock, J. (2022). *Understand the Mistakes that compromise your Company's Cybersecurity*. Tessian. https://www.tessian.com/research/the-psychology-of-human-error/

Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, *45*(4), 534-567. https://doi.org/10.1080/01402390.2020.1732354

Hartwig, K., & Reuter, C. (2021). Nudge or restraint: How do people assess nudging in cybersecurity - A representative study in Germany. *ACM International Conference Proceeding Series*, 141-150. https://doi.org/10.1145/3481357.3481514

Hatta, M. (2020). Deep web, dark web, dark net. *Annals of Business Administrative Science*, *19*(6), 277-292. https://doi.org/10.7880/ABAS.0200908A

Hausman, D. M., & Welch, B. (2010). Debate: To nudge or not to nudge. *Journal of Political Philosophy*, *18*(1), 123-136.

Healey, J. (2012). *Beyond Attribution: Seeking National Responsibility in Cyberspace*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/

Hern, A. (2021). *Fastly says single customer triggered bug behind mass internet outage*. The Guardian. Retrieved Oct 29, 2023 from https://www.theguardian.com/technology/2021/jun/09/fastly-says-single-customer-triggered-bug-that-caused-mass-outage

Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. *Royal Society Open Science*, *7*, 190023. https://doi.org/10.1098/rsos.190023

Herrmann, D., & Pridöhl, H. (2020). Basic Concepts and Models of Cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (pp. 11-44). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5_2

Hewitt, B., & White, G. L. (2022). Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *The Journal of computer information systems*, *62*(1), 50-60. https://doi.org/10.1080/08874417.2019.1697860

Hielscher, J., Menges, U., Parkin, S., Kluge, A., & Sasse, M. A. (2023). "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. 32st USENIX Security Symposium (USENIX Security 23), Aug 9-11, Boston, MA, USA.

Hodgkinson, G. P., Bown, N. J., Maule, A. J., Glaister, K. W., & Pearman, A. D. (1999). Breaking the frame: An analysis of strategic cognition and decision making under uncertainty. *Strategic Management Journal*, *20*(10), 977-985.

Hofmann, J. (2010). *The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia*.

Hofmans, T. (2018). *Teenager suspected of crippling Dutch banks with DDoS attacks* ComputerWeekly. Retrieved Nov 5, 2023 from https://www.computerweekly.com/news/252434665/Teenager-suspected-of-crippling-Dutch-banks-with-DDoS-attacks

Hojda, M. (2022). Information security economics: cyber security threats. *Proceedings of the International Conference on Business Excellence*, *16*, 584-592. https://doi.org/10.2478/picbe-2022-0056

Holland, S., & Pearson, J. (2022). *US, UK: Russia responsible for cyberattack against Ukrainian banks*. Reuters. Retrieved Dec 7, 2023 from https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/

Holt, T. (2017). Limitations and Possibilities of estimating the Costs of Cybercrime. *Cyber Infrastructure Protection Volume III. Strategic Studies Institute. US Army War College*, 35-65.

Holt, T., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, *6*.

Hong, Y., Kim, M.-J., & Roh, T. (2023). Mitigating the Impact of Work Overload on Cybersecurity Behavior: The Moderating Influence of Corporate Ethics—A Mediated Moderation Analysis. *Sustainability*, *15*, 14327. https://doi.org/10.3390/su151914327

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585-591.

Hope, A. (2020). *New Zealand Stock Exchange Shut Down by DDoS Cyber Attack*. Retrieved Aug 21, 2023 from https://www.cpomagazine.com/cyber-security/new-zealand-stock-exchange-shut-down-by-ddos-cyber-attack/

Hovav, A., & D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*, 97-121. https://doi.org/10.1046/J.1098-1616.2003.026.x

Howell O'Neill, P. (2020). *Ransomware did not kill a German hospital patient*. Retrieved Aug 21, 2023 from https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/

Huang, K., & Madnick, M. S. S. (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Survey. *ACM Comput. Surv.*, *51*(4), Article 70. https://doi.org/10.1145/3199674

Huang, K., Wang, X., Wei, W., & Madnick, S. (2023). *The devastating business impacts of a cyber breach*. Harvard Business Review. Retrieved Jul 31, 2024 from https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review*, *28*(2), 201-207. https://doi.org/10.1016/J.CLSR.2012.01.007

Hunziker, S., & Fallegger, M. (2019). *Erfolgsfaktor Mensch im Enterprise Risk Management – Teil 7: Affektheuristik*. University Luzern. Retrieved Nov 4, 2023 from https://hub.hslu.ch/financialmanagement/2019/05/09/erfolgsfaktor-mensch-im-enterprise-risk-management-teil-7-affektheuristik/

IBM. (2021). *SPSS Statistics (Version 21) [Computer software]*. https://www.ibm.com/de-de/products/spss-statistics

IBM/Ponemon Institute. (2022). *Cost of a Data Breach Report 2022*. https://www.ibm.com/downloads/cas/3R8N1DZJ

ICE. (2013). *HSI seizes biggest anonymous drug black market website and assists in arrest of operator and overseas co-conspirators*. U.S. Immigration and Customs Enforcement (ICE) Retrieved Aug 24, 2023 from https://www.ice.gov/news/releases/hsi-seizes-biggest-anonymous-drug-black-market-website-and-assists-arrest-operator

IDC. (2021). *IDC Forecasts Worldwide "Whole Cloud" Spending to Reach $1.3 Trillion by 2025*. Retrieved Jun 25, 2023 from https://www.businesswire.com/news/home/20210914005759/en/IDC-Forecasts-Worldwide-Whole-Cloud-Spending-to-Reach-1.3-Trillion-by-2025

IDC. (2023). *New IDC Spending Guide Forecasts Worldwide Security Investments Will Grow 12.1% in 2023 to $219 Billion*. Retrieved Oct 4, 2023 from https://www.idc.com/getdoc.jsp?containerId=prUS50498423

Insights, H. (2022). *Revealed: The AWS Ecosystem In 2022*. Retrieved Aug 22, 2023 from https://hginsights.com/market-reports/hg-insights-intricately-aws-ecosystem-report-in-2022

Interpol. (2023). *USD 300 million seized and 3,500 suspects arrested in international financial crime operation*. Retrieved Dec 21, 2023 from https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

Isidore, C. (2016). *Delta: 5-hour computer outage cost us $150 million*. CNN. Retrieved Dec 1, 2023 from https://money.cnn.com/2016/09/07/technology/delta-computer-outage-cost/

Islam, M. S., Wang, T., Farah, N., & Stafford, T. (2022). The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume. *Journal of Accounting and Public Policy*, *41*(2). https://doi.org/10.1016/J.JACCPUBPOL.2021.106916

ITU. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*.

ITU. (n. d.). *Statistics*. Retrieved May 29, 2024 from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx#:~:text=Statistics%20ITU%20estimates%20that%

20approximately%204.9%20billion%20people,estimated%20to%20have%20come%20online%20during%20that%20period.?msclkid=629fc24bb64011ec9c6f0a707ec8a656

Jaeger, J. (2020). *Equifax must spend 'a minimum of $1B' for data security*. Compliance Week. Retrieved Oct 13, 2023 from https://www.complianceweek.com/cybersecurity/equifax-must-spend-a-minimum-of-1b-for-data-security/28329.article

Jain, A. (2014). Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine. *Chicago-Kent Journal of International and Comparative Law*, *14*(2). https://scholarship.kentlaw.iit.edu/ckjicl/vol14/iss2/2

Jakobi, A. (2013). Non-state actors all around: The governance of cybercrime. In A. P. Jakobi & K. D. Wolf (Eds.), *The Transnational Governance of Violence and Crime.* (pp. 129-148). Palgrave Macmillan. https://pure.royalholloway.ac.uk/en/publications/non-state-actors-all-around-the-governance-of-cybercrime

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66-82. https://doi.org/10.1016/j.jsis.2018.09.003

James, R., & Kim, S. N. (2023). *Security Chiefs Trim the Fat as Budgets Bite*. The Wall Street Journal. Retrieved Oct 2, 2023 from https://www.wsj.com/articles/security-chiefs-trim-the-fat-as-budgets-bite-83c82f99

Jayakumar, S. (2021). Cyber Attacks By Terrorists And Other Malevolent Actors: Prevention and Preparedness. *Home Team Journal*(11). https://www.icct.nl/sites/default/files/2023-01/Chapter-29-Handbook-.pdf

Jeffray, C., & Feakin, T. (2015). *Underground web : the cybercrime challenge*.

Jensen, B. (2017). The Cyber Character of Political Warfare. *The Brown Journal of World Affairs*, *24*(1). https://www.jstor.org/stable/27119085

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681-695. https://doi.org/10.1016/j.im.2018.11.003

Ji-Young, K. e. a. (2019). *The All-Purpose Sword: North Korea's Cyber Operations and Strategies* 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Johnson, C. K., Gutzwiller, R. S., Ferguson-Walter, K. J., & Fugate, S. J. (2020). *A cyber-relevant table of decision making biases and their definitions*.

Johnson, E. J., & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology*, *45*(1), 20-31. https://doi.org/10.1037/0022-3514.45.1.20

Johnson, M., Kang, M. J., & Lawson, T. (2017). Stock Price Reaction to Data Breaches. Journal of Finance Issues. *Journal of Finance Issues*, *16*(2), 1-13. https://doi.org/10.58886/jfi.v16i2.2263

Jöreskog, K. G., & Sörbom, D. (1982). Recent Developments in Structural Equation Modeling. *Journal of Marketing Research*, *19*(4), 404-416. https://doi.org/10.1177/002224378201900402

Kadlecová, L. (2015). Russian-speaking Cyber Crime: Reasons behind Its Success. *The European Review of Organised Crime*, *2*(2), 104-121. https://www.academia.edu/16548880/Russian_speaking_Cyber_Crime_Reasons_behind_Its_Success

Kagan, D., Alpert, G. F., & Fire, M. (2020). Zooming into video conferencing privacy and security threats. *arXiv preprint arXiv:2007.01059*. https://doi.org/10.48550/arXiv.2007.01059

Kahneman, D. (2003). Maps of Bounded Rationality: Psychology for Behavioral Economics †. *American Economic Review*, *93*, 1449-1475. https://doi.org/10.1257/000282803322655392

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias. *Journal of Economic Perspectives*, *5*(1), 193-206. https://doi.org/10.1257/jep.5.1.193

Kahneman, D., Lovallo, D., & Sibony, O. (2011). Before you make that big decision. *Harvard Business Review*, *89*, 50-60, 137.

Kahneman, D., & Tversky, A. (1974). Subjective Probability: A Judgment of Representativeness. In C.-A. S. Stael Von Holstein (Ed.), *The Concept of Probability in Psychological Experiments* (pp. 25-48). Springer. https://doi.org/10.1007/978-94-010-2288-0_3

Kapto, A. S. (2013). Cyberwarfare: Genesis and doctrinal outlines. *Herald of the Russian Academy of Sciences*, *83*(4), 357-364. https://doi.org/10.1134/s1019331613040023

Karuppannan, J. (2009). Space Transition Theory of Cyber Crimes. In M. P. Frank Schmalleger (Ed.), *Crimes of the Internet* (pp. 283-301). Prentice Hall.

Keane, M. P., & Thorp, S. (2016). Chapter 11 - Complex Decision Making: The Roles of Cognitive Limitations, Cognitive Decline, and Aging. In J. Piggott & A. Woodland (Eds.), *Handbook of the Economics of Population Aging* (Vol. 1, pp. 661-709). North-Holland. https://doi.org/10.1016/bs.hespa.2016.09.001

Keary, T. (2022). *Twitter API security breach exposes 5.4 million users' dataexposes 5.4 million users' data*. Venture Beat. Retrieved Oct 5, 2023 from https://venturebeat.com/security/twitter-breach-api-attack/

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft on JSTOR. *International Security*, *38*(2), 7-40. https://www.jstor.org/stable/24480929

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293-312. https://doi.org/10.1007/S10610-020-09439-2

Khan, L. M. (2017). Amazon's Antitrust Paradox. *The Yale Law Journal*, *126*(3), 710-805.

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Trans. Priv. Secur.*, *26*(1), Article 3. https://doi.org/10.1145/3546068

Khorrami, N. (2022). *Amid ongoing protests, Iran is looking to accelerate its adoption of China's AI surveillance and internet censorship methods*. Retrieved Jul 2, 2023 from https://thediplomat.com/2022/10/how-china-boosts-irans-digital-crackdown

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(24), 13677. https://www.mdpi.com/2071-1050/13/24/13677

Kianpour, M., Øverby, H., Kowalski, S., & Frantz, C. (2019). Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties. In (pp. 149-163). https://doi.org/10.1007/978-3-030-22351-9_10

Kim, H.-W., & Kankanhalli, A. (2009). Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective. *MIS Quarterly*, *33*, 567-582. https://doi.org/10.2307/20650309

Kim, M.-H. (2022). North Korea's Cyber Capabilities and Their Implications for International Security. *Sustainability*, *14*(3), 1744. https://doi.org/10.3390/su14031744

Kleinewiese, J. (2022). The Darkfield of Cybercrime: Can Survey Data Reduce Administrative Data's Problem with Validity? *International Journal of Cyber Criminology*, *16*, 141-155. https://doi.org/10.5281/zenodo.4766561

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, *58*, 39-46. https://doi.org/10.1016/J.COSE.2015.12.001

Koren, D., Kilar, V., & Rus, K. (2017). *Proposal for Holistic Assessment of Urban System Resilience to Natural Disasters* Sep 21-22, IOP Conference Series: Materials Science and Engineering, Prague, Czech Republic. http://dx.doi.org/10.1088/1757-899X/245/6/062011

Kostyuk, N., & Wayne, C. (2020). The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies*, *6*(2). https://doi.org/10.1093/jogss/ogz077

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors Related to Cyber Security Behavior. *Ieee Access*, *8*, 125140-125148. https://doi.org/10.1109/ACCESS.2020.3007867

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541-555. https://doi.org/10.1016/J.TECHFORE.2012.07.002

Krasznay, C. (2020). Case Study: The NotPetya Campaign. In *Információ- és kiberbiztonság* (pp. 485-499). Ludovika Egyetemi Kiadó.

Krawczyk, D., Bartlett, J., Kantarcioglu, M., Hamlen, K., & Thuraisingham, B. (2013). *Measuring expertise and bias in cyber security using cognitive and neuroscience approaches* IEEE International Conference on Intelligence and Security Informatics, Seattle, WA, USA.

Kremer, J. F., & Müller, B. (2014). *Cyberspace and international relations: Theory, prospects and challenges*. Springer-Verlag. https://doi.org/10.1007/978-3-642-37481-4

Kropotov, V., McArdle, R., & Yarochkin, F. (2020a). *The Hacker Infrastructure and Underground Hosting: Cybercrime Modi Operandi and OpSec*. https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting.pdf

Kropotov, V., McArdle, R., & Yarochkin, F. (2020b). *The Hacker Infrastructure and Underground Hosting: Services Used by Criminals*. https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting-services-used-by-criminals.pdf

Kruger, J., & Gilovich, T. (1999). Naive Cynicism in Everyday Theories of Responsibility Assessment: On Biased Assumptions of Bias. *Journal of Personality and Social Psychology*, *76*, 743-753. https://doi.org/10.1037/0022-3514.76.5.743

Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, 1-251. https://doi.org/10.1007/978-3-642-11522-6/COVER

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China. *Electronic Commerce Research*, *13*(1), 41-69. https://doi.org/10.1007/S10660-013-9105-4

Kshetri, N. (2014). Cyberwarfare in the Korean peninsula: Asymmetries and strategic responses. *East Asia*, *31*(3), 183-201. https://doi.org/10.1007/S12140-014-9215-1

Kshetri, N. (2016). Cybersecurity in Russia. In *The Quest to Cyber Superiority* (pp. 211-221). Springer, Cham. https://doi.org/10.1007/978-3-319-40554-4_13

Kuckartz, U. (2014). *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software*. Sage Publications Ltd. https://doi.org/10.4135/9781446288719

Kumar, A. R., E. (2019). *The Truth about the DarkWeb*. https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219-236. https://doi.org/10.2308/isys-50339

Lahcen, R., Mohapatra, R., & Kumar, M. (2018). Cybersecurity: A survey of vulnerability analysis and attack graphs. Mathematics and Computing: ICMC 2018, Jan 9-11, Varanasi, India.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*. https://doi.org/10.1016/J.COSE.2021.102248

Langley, A., Mintzberg, H., Pitcher, P., Posada, E., & Saint-Macary, J. (1995). Opening up Decision Making: The View from the Black Stool. *Organization Science*, *6*(3), 260-279. http://www.jstor.org/stable/2635251

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*(6), 321-330.

Le, N. T., & Hoang, D. B. (2017). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016*. https://doi.org/10.1109/PCCC.2016.7820663

Lemay, A., & Leblanc, S. (2018). Cognitive biases in cyber decision-making. Proceedings of the 13th International Conference on Cyber Warfare and Security, Mar 8-9, Washington, DC, USA.

Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., & Cranor, L. (2012). Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/2207676.2207759

Lerman, R., & Vynck, G. D. (2021). *Ransomware claims are roiling an entire segment of the insurance industry*. The Washington Post. Retrieved Dec 2, 2023 from https://www.washingtonpost.com/technology/2021/06/17/ransomware-axa-insurance-attacks/

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*. https://doi.org/10.1016/J.CHB.2021.106979

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change. *Crime, Law and Social Change*, *67*(1), 3-20. https://doi.org/10.1007/S10611-016-9645-3

Levi, M., & Smith, R. G. (2021). *Fraud and its relationship to pandemics and economic crises: from Spanish flu to COVID-19*. Australian Institute of Criminology.

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies*. https://www.steptoe.com/a/web/4586/231a.pdf

Lewis, J. A. (2018). *Economic Impact of Cybercrime*. https://www.csis.org/analysis/economic-impact-cybercrime

Li, W., Chen, H., & Nunamaker, J. (2016). Identifying and Profiling Key Sellers in Cyber Carding Community: AZSecure Text Mining System. *Journal of Management Information Systems*, *33*, 1059-1086. https://doi.org/10.1080/07421222.2016.1267528

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/J.EGYR.2021.08.126

Lillis, K. B., & Lyngaas, S. (2021). *Cyber Command head says US has carried out a 'surge' to address ransomware attacks* CNN. Retrieved Aug 18, 2023 from https://edition.cnn.com/2021/11/03/politics/nakasone-ransomware-surge/index.html

Limnéll, J. (2018). Developing political response framework to cyber hostilities. *Intelligent Systems, Control and Automation: Science and Engineering*, *93*, 31-48. https://doi.org/10.1007/978-3-319-75307-2_3

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review*, *5*(19), 24-47.

Lizarraga, M., Baquedano, M. T., Soria-Oliver, M., & Closas, A. (2009). Development and Validation of a Decision-Making Questionnaire. *British Journal of Guidance & Counselling*, *37*. https://doi.org/10.1080/03069880902956959

Lloyds of London. (2018). *Cloud down*. https://www.lloyds.com/clouddown

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2022). Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective. *IEEE Transactions on Engineering Management*, *69*(6), 3757-3770. https://doi.org/10.1109/TEM.2020.2996175

Lowry, M. R., Sahin, Z., & Vance, A. (2022). Taking a Seat at the Table: The Quest for CISO Legitimacy.

Lu, D., & Kurmelovs, R. (2022). *Optus data breach: cybersecurity reforms expected to enable companies to rapidly inform financial institutions*. The Guardian. Retrieved Oct 5, 2023 from https://www.theguardian.com/business/2022/sep/25/optus-data-breach-cybersecurity-reforms-expected-to-enable-companies-to-rapidly-inform-financial-institutions

Lu, J. (2019). Assessing the cost, legal fallout of Capital One data breach. *Law360 Expert Analysis*.

Lynch, D. (2017). *Ex-Equifax boss details errors behind data breach*. Financial Times. Retrieved Oct 12, 2023 from https://www.ft.com/content/1c23b11c-a857-11e7-ab55-27219df83c97

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 10. https://doi.org/10.1186/s42400-020-00050-w

Maillart, J. B. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum*, *19*(3), 375-390. https://doi.org/10.1007/S12027-018-0527-2/METRICS

Mancuso, V., Funke, G. J., Finomore, V., & Knott, B. A. (2013). Exploring the Effects of "Low and Slow" Cyber Attacks on Team Decision Making. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 389-393. https://doi.org/10.1177/1541931213571084

Maness, R. C., & Valeriano, B. (2016). Cyber spillover conflicts. In F. Karsten & R. Jens (Eds.), *Conflict in Cyber Space* (1st Edition ed.). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315669878-4/cyber-spillover-conflicts-ryan-maness-brandon-valeriano

Mangan, D. (2023). *'Fraud is fun' DraftKings teen hacker pleads guilty in fantasy sports betting theft*. Retrieved Dec 11, 2023 from https://www.cnbc.com/2023/11/15/fraud-is-fun-draft-kings-hacker-pleads-guilty-in-fantasy-sports-betting-case.html

Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud and Security*, *2013*(6), 9-13. https://doi.org/10.1016/S1361-3723(13)70053-8

Maras, M.-H. (2016). *Cybercriminology*. Oxford University Press.

Marsh/Microsoft. (2018). *By the Numbers: Global Cyber Risk Perception Survey* https://www.marsh.com/kr/en/services/cyber-risk/insights/global-cyber-risk-perception-survey.html

Martin, J. (2014). Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs. *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*, 1-92. https://doi.org/10.1057/9781137399052

Martin, T. (2018). *North Korea, While Professing Peace, Escalated Cyberattacks on South*. The Wall Street Journal. Retrieved Jul 1, 2023 from https://www.wsj.com/articles/north-korea-while-professing-peace-escalated-cyberattacks-on-south-1527239057

Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., Lioy, A., López, D., Santos, H., & Gonos, A. (2021). Cybersecurity in ICT supply chains: key challenges and a relevant architecture. *Sensors*, *21*(18), 6057.

Mathis, K., & Steffen, A. D. (2015). From Rational Choice to Behavioural Economics. In K. Mathis (Ed.), *European Perspectives on Behavioural Law and Economics* (pp. 31-48). Springer International Publishing. https://doi.org/10.1007/978-3-319-11635-8_3

Mavuduru, A. (2020). *Is Data Really the New Oil in the 21st Century?* Towards Data Science. Retrieved Jun 20, 2023 from https://towardsdatascience.com/is-data-really-the-new-oil-in-the-21st-century-17d014811b88

Maynard, S., Onibere, M., & Ahmad, A. (2018). Defining the strategic role of the chief information security officer. *Pacific Asia Journal of the Association for Information Systems*, *10*(3), 3.

McCaskill, N. (2016). *Trump: It's time 'to move on' from claims of Russian interference in election*. Politico. Retrieved Aug 11, 2023 from https://www.politico.com/story/2016/12/trump-russian-cyberattacks-intelligence-233045

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. A., & Pattinson, M. R. (2017). Individual differences and Information Security Awareness. *Comput. Hum. Behav.*, *69*, 151-156.

McCrindle, M. F., A. (2020). *Understanding Generation Alpha*. https://generationalpha.com/wp-content/uploads/2020/02/Understanding-Generation-Alpha-McCrindle.pdf

McGregor, R., Reaiche, C., Boyle, S., & Corral de Zubielqui, G. (2023). Cyberspace and Personal Cyber Insurance: A Systematic Review. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2023.2185551

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence Research Report 75 Chapter 1: Cyber-dependent crimes*.

McLaughlin, J. (2022). *Ukraine says government websites and banks were hit with denial of service attack*. Retrieved Aug 18, 2023 from https://www.npr.org/2022/02/15/1080876311/ukraine-hack-denial-of-service-attack-defense

Medeiros, B. P., & Goldoni, L. R. F. (2020). The Fundamental Conceptual Trinity of Cyberspace. *Contexto Internacional*, *42*(1), 31-54. https://doi.org/10.1590/S0102-8529.2019420100002

Mehrabi, R. (2012). Investigating Effect of Entrepreneur's Personal Attributes and Cognitive Heuristics on the Quality of Entrepreneurial Strategic Decision Making. *Global Business and Management Research: An International Journal*, *4*, 178.

Mehta, I. (2019). *The Need for Better Metrics on Cybercrime*. http://www.jstor.com/stable/resrep20149

Meijer, B. H., & Siebold, S. (2022). *'Pro-Russia' hackers down EU Parliament website for hours*. Reuters. Retrieved Dec 8, 2023 from https://www.reuters.com/world/europe/pro-kremlin-group-says-responsible-cyberattack-eu-parliament-official-2022-11-23/

Mellers, B., Schwartz, A., & Ritov, I. (1999). Emotion-based choice. *Journal of Experimental Psychology: General*, *128*(3), 332.

Microsoft. (2021). *Iranian targeting of IT sector on the rise*. Retrieved Jun 29, 2023 from https://www.microsoft.com/en-us/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise

Miller, M. (2020). *FBI sees spike in cyber crime reports during coronavirus pandemic* The Hill. Retrieved Nov 24, 2023 from https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/

Milliard, M. (2021). *Boston Children's Hospital was target of cyberattack thwarted by FBI*. Retrieved Aug 21, 2023 from https://www.healthcareitnews.com/news/boston-childrens-hospital-was-target-cyberattack-thwarted-fbi

Mintzberg, H., Raisinghani, D., & Théorêt, A. (1976). The Structure of "Unstructured" Decision Processes. *Administrative Science Quarterly*, *21*(2), 246-275. https://doi.org/10.2307/2392045

Mintzberg, H., & Waters, J. A. (1982). Tracking strategy in an entrepreneurial firm. *Academy of management journal*, *25*(3), 465-499.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, *58*(1), 7-38. https://doi.org/10.1080/00396338.2016.1142085

Moore, D. A., & Healy, P. J. (2008). The trouble with overconfidence. *Psychological Review*, *115*(2), 502-517. https://doi.org/10.1037/0033-295X.115.2.502

Moore, J. F. (1993). Predators and Prey: A New Ecology of Competition. *Harvard Business Review*, *71*(3), 75-86. https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3), 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

Moraski, L. (2011). Cybercrime knows no borders. *Infosecurity*, *8*(2), 20-23. https://doi.org/10.1016/S1754-4548(11)70021-3

Moulson, G. (2019). *Germany shuts down illegal data center in former NATO bunker*. Retrieved Aug 27, 2023 from https://apnews.com/article/nato-technology-crime-europe-germany-be9947471fb74360b6cf9d1d2b535927

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011.

Mueller, P., & Yadegari, B. (2012). The Stuxnet Worm. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

Mullen, J., & Fiegerman, S. (2017). *Yahoo tops the list of largest ever data breaches*. CNN. Retrieved Oct 13, 2023 from https://money.cnn.com/2017/10/04/technology/yahoo-biggest-data-breaches-ever/index.html

Muncaster, P. (2023). *Killnet Attackers DDoS US and Dutch Hospitals*. Retrieved Aug 21, 2023 from https://www.infosecurity-magazine.com/news/killnet-suspected-ddos-us-dutch/

Murphy, H. (2021). *Monero emerges as crypto of choice for cybercriminals*. Financial Times. Retrieved Aug 14, 2023 from https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6

Myburgh, W., Watson, M., & Foxcroft, C. (2015). Development and validation of a managerial decision making self-efficacy questionnaire. *SA Journal of Industrial Psychology*, *41*. https://doi.org/10.4102/sajip.v41i1.1218

NATO. (2023). *Countering Hybrid Threats*. Retrieved Jul 18, 2023 from https://www.nato.int/cps/en/natohq/topics_156338.htm

Nayak, M., & Narayan, K. A. (2019). Strengths and Weakness of Online Surveys. *24*, 31-38. https://doi.org/10.9790/0837-2405053138

NCSC. (2018). *Russian military 'almost certainly' responsible for destructive 2017 cyber attack*. Retrieved Aug 19, 2023 from https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

NCSC. (2023). *NCSC joins partners to issue warning about China state-sponsored cyber activity targeting CNI networks*. Retrieved Nov 22, 2023 from https://www.ncsc.gov.uk/news/ncsc-joins-partners-to-issue-warning-about-chinese-cyber-activity-targeting-cni

Neckermann, J. (2020). Over-Confidence Bias in strategischen Entscheidungsprozessen: Entstehung, Konsequenzen und Lösungsansätze. *Junior Management Science*, *5*(3), 392-409.

Ng, K. (2023). *Crypto theft: North Korea-linked hackers stole $1.7b in 2022*. BBC. Retrieved Jul 8, 2023 from https://www.bbc.com/news/world-asia-64494094

Nguyen, M., Bin, Y. S., & Campbell, A. (2012). Comparing Online and Offline Self-Disclosure: A Systematic Review. *Cyberpsychology, Behavior, and Social Networking*, *15*(2), 103-111. https://doi.org/10.1089/cyber.2011.0277

Nikkhah, H. R., & Grover, V. (2022). An Empirical Investigation of Company Response to Data Breaches. *MIS Quarterly*, *46*, 2163-2196. https://doi.org/10.25300/MISQ/2022/16609

NIST. (2021). *Defending Against Software Supply Chain Attacks*. https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

NIST. (n. d.-a). *Cyber Resiliency*. Retrieved Sep 2, 2023 from https://csrc.nist.gov/glossary/term/cyber_resiliency

NIST. (n. d.-b). *Risk Management Framework (RMF)*. Retrieved Sep 2, 2023 from https://csrc.nist.gov/projects/risk-management/about-rmf

Nobles, C., Burton, S. L., & Burrell, D. (2023). Cybercrime as a sustained business. *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems*, 98-120. https://doi.org/10.4018/978-1-6684-7207-1.CH005

Nolan, C., & Fixler, A. (2021). *The Economic Costs of Cyber Risk*.

Noroozian, A., Korczyński, M., Gañan, C. H., Makita, D., Yoshioka, K., & Vaneeten, M. (2016). Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9854 LNCS*, 368-389. https://doi.org/10.1007/978-3-319-45719-2_17

Novaes Neto, N., Madnick, S., de Paula, A., & Malara Borges, N. (2020). *A Case Study of the Capital One Data Breach (Revised)*.

Nuijten, A., Benschop, N., Rijsenbilt, A., & Wilmink, K. (2020). Cognitive Biases in Critical Decisions Facing SME Entrepreneurs: An External Accountants' Perspective. *Administrative Sciences*, *10*(4), 89. https://www.mdpi.com/2076-3387/10/4/89

Nuryana, Z., Pangarso, A., & Zain, F. M. (2021). Factor of Zoom Cloud Meetings: Technology Adoption in the Pandemic of COVID-19. *International Journal of Evaluation and Research in Education*, *10*(3), 816-825.

Ocean Tomo. (2020). *Intangible Asset Market Value Study*. https://oceantomo.com/intangible-asset-market-value-study/

Office for National Statistics. (2022). *Crime in England and Wales: year ending September 2021 - Office for National Statistics*. Retrieved Jul 13, 2023 from https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingseptember2021

Olmstead, K., & Smith, A. (2017a). *Americans and Cybersecurity*. Pew Research Center.

Olmstead, K., & Smith, A. (2017b). *What the Public Knows About Cybersecurity*. Pew Research Center.

Ottis, R., & Lorents, P. (2013). Cyberspace: Definition and Implications - ProQuest. *5th European Conference on Information Management and Evaluation*, 267-270. https://www.proquest.com/docview/869617247?pq-origsite=gscholar/

Ouellet, F., & Dubois, M. È. (2022). Got assistance? Profit-driven criminal careers and assisted desistance. *Crime and delinquency*. https://doi.org/10.1177/00111287221104733

Ouellet, M., Décary-Hétu, D., & Bergeron, A. (2022). Cryptomarkets and the Returns to Criminal Experience. *CSLF Articles*. https://scholarworks.gsu.edu/ays_cslf_articles/3

Paek, H.-J., & Hove, T. (2017). Risk Perceptions and Risk Characteristics. In: Oxford University Press.

Pape, C. (2022). *10 biggest financial data breaches of 2022*. Retrieved Nov 5, 2023 from https://www.americanbanker.com/list/10-biggest-financial-data-breaches-of-2022

Pareto, V. (2014). *Manual of Political Economy: A Critical and Variorum Edition* (A. Montesano, A. Zanni, L. Bruni, J. S. Chipman, & M. McLure, Eds.). Oxford University Press.

Park, J., Cho, D., Lee, J., & Lee, B. (2019). The Economics of Cybercrime. *ACM Transactions on Management Information Systems (TMIS)*, *10*(4). https://doi.org/10.1145/3351159

Peppard, J., & Ward, J. (2016). *The Strategic Management of Information Systems: Building a Digital Strategy* (4th ed.). John Wiley & Sons.

Peters, A., & Jordan, A. (2020). Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. *Journal of National Security Law & Policy 10*(3).

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597-611. https://doi.org/10.1016/J.COSE.2011.12.010

Pijpers, P. B. M. J. (2023). *Influence operations in cyberspace and the applicability of international law*. Edward Elgar Publishing. https://www.e-elgar.com/shop/gbp/influence-operations-in-cyberspace-and-the-applicability-of-international-law-9781035307289.html

Pitney Bowes. (2022). *Parcel Shipping Index 2022*. https://www.pitneybowes.com/content/dam/pitneybowes/us/en/shipping-index/22-pbcs-04529-2021-global-parcel-shipping-index-ebook-web-002.pdf

Pollitt, M. (1997). *A Cyberterrorism Fact or Fancy?* Proceedings of the 20th National Information Systems Security Conference, Oct 7-10, Baltimore, MD, USA.

Ponemon Institute. (2016). *Cost of Data Center Outages*. https://www.ponemon.org/research/ponemon-library/security/2016-cost-of-data-center-outages.html

Porche, I. (2019). *Cyberwarfare: an introduction to information-age conflict*. Artech House.

Porter, S. (2020). *Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak*. Retrieved Aug 21, 2023 from https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak

Potamos, G., Theodoulou, S., Stavrou, E., & Stavrou, S. (2023). Building Maritime Cybersecurity Capacity Against Ransomware Attacks, in: Onwubiko, C. et al. (2023). Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Springer Proceedings in Complexity.

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

Pratama, A. R., & Firmansyah, F. M. (2021). Until you have something to lose! Loss aversion and two-factor authentication adoption. *Applied Computing and Informatics*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ACI-12-2020-0156

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296. https://doi.org/10.1177/0022427810365903

Prieto Curiel, R., Collignon Delmar, S., & Bishop, S. R. (2018). Measuring the Distribution of Crime and Its Concentration. *Journal of Quantitative Criminology*, *34*(3), 775-803. https://doi.org/10.1007/S10940-017-9354-9/TABLES/7

Prior, R. (2019). *Equifax will pay up to $700 million over its data breach. Here's how to claim your money.* CNN. Retrieved Oct. 12, 2023 from https://edition.cnn.com/2019/07/25/us/equifax-700-million-settlement-data-breach-trnd/index.html

PrivacyAffairs. (n. d.). Retrieved Jun 26, 2023 from https://www.privacyaffairs.com/dark-web-price-index-2023/

Probasco, J. R., & Davis, W. L. (1995). A human capital perspective on criminal careers. *Journal of Applied Business Research*, *11*(3), 58-64.

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

Pursiainen, C., & Forsberg, T. (2021). The Cognitive Limitations of Rationality. In *The Psychology of Foreign Policy* (pp. 47-87). Springer International Publishing. https://doi.org/10.1007/978-3-030-79887-1_2

PwC. (2023). *A C-suite united on cyber-ready futures - Findings from the 2023 Global Digital Trust Insights*. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

Qu, L., Wang, C., Xiao, R., Hou, J., Shi, W., & Liang, B. (2019). *Towards Better Security Decisions: Applying Prospect Theory to Cybersecurity* Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, May 4-9, Glasgow, United Kingdom. https://doi.org/10.1145/3290607.3312782

Radziwill, Y. (2015). *Cyber-Attacks and the Exploitable Imperfections of International Law*. Brill Nijhoff. https://doi.org/10.1163/9789004298309

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). *Human Factors in Cybersecurity: A Scoping Review* Proceedings of the 12th International Conference on Advances in Information Technology, Jun 29-Jul 1, Bangkok, Thailand. https://doi.org/10.1145/3468784.3468789

Reuters. (2021). *U.S. spied on Merkel and other Europeans through Danish cables*. Retrieved Jul 9, 2023 from https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online:Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169. https://doi.org/10.1177/0093854811421448

Rhee, H.-S., Ryu, Y., & Kim, C. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. International Conference on Information Systems (ICIS), Dec 11-14, Las Vegas, NV, USA.

Rhee, H.-S., Ryu, Y., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*, 221–232. https://doi.org/10.1016/j.cose.2011.12.001

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention.

Riley, C. (2019). *British Airways faces $230 million fine. It would be a record under Europe's tough data privacy law*. CNN. Retrieved Aug 23, 2023 from https://edition.cnn.com/2019/07/08/tech/british-airways-gdpr-fine/index.html

Robinson, A. e. a. (2022). *New Risks in Ransomware: Supply Chain Attacks and Cryptocurrency*. https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37373233

Rodriguez-Priego, N., & Bavel, R. v. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services*, *72*(C). https://doi.org/10.1016/j.jretconser.2023

Rohan, R., Funilkul, S., Pal, D., & Chutimaskul, W. (2021). Understanding of human factors in cybersecurity: A systematic literature review. 2021 International Conference on Computational Performance Evaluation (ComPE), Dec 1-3, Online.

Rosengren, O. (2023). *APT Networks: A Force Multiplier in China's Push for Global Power*. Retrieved Jul 12, 2023 from https://greydynamics.com/apt-networks-a-force-multiplier-in-chinas-push-for-global-power

Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, *33*(4), 517-529. https://doi.org/10.1007/s10669-013-9473-2

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12-15.

Ruiz, R., Winter, R., Park, K., & Amatte, F. (2015). Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *4*, 404-416. https://doi.org/10.17781/P001619

Rundle, J. (2019). *Human Error Often the Culprit in Cloud Data Breaches*. The Wall Street Journal. Retrieved Oct 12, 2023 from https://www.wsj.com/articles/human-error-often-the-culprit-in-cloud-data-breaches-11566898203

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K.-K. R., & Al-Qirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, *9*(1), 211-222. https://doi.org/10.1016/j.dcan.2022.06.005

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty*, *1*(1), 7-59. https://doi.org/10.1007/BF00055564

Santanna, J. J., Van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). Booters - An analysis of DDoS-as-a-service attacks. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 243-251. https://doi.org/10.1109/INM.2015.7140298

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330. https://doi.org/10.1016/j.techfore.2015.08.012

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers*, *19*(5), 1205-1228. https://doi.org/10.1007/S10796-016-9648-8

Scherbina, A. D., & Schlusche, B. (2023). The Effect of Malicious Cyber Activity on the U.S. Corporate Sector. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.4400066

Schiffer, A. (2017). *How a fish tank helped hack a casino*. The Washington Post. Retrieved Aug 16, 2023 from https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Schiks, J. A. M., van de Weijer, S. G. A., & Leukfeldt, E. R. (2022). High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals. *Computers in Human Behavior*, *126*, 106985-106985. https://doi.org/10.1016/J.CHB.2021.106985

Schneider, F., Raczkowski, K., & Mróz, B. (2015). Shadow economy and tax evasion in the EU. *Journal of Money Laundering Control*, *18*(1), 34-51.

Schrager, J. E., & Madansky, A. (2013). Behavioral strategy: a foundational view. *Journal of Strategy and Management*, *6*(1), 81-95.

Schwarcz, S. L. (2008). Systemic Risk. *Georgetown Law Journal*, *97*(1). https://papers.ssrn.com/abstract=1008326

Schwarz, N. (2002). Feelings as Information: Moods Influence Judgments and Processing Strategies. In T. Gilovich, D. Griffin, & D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive judgment* (pp. 534-547). Cambridge U Press. https://doi.org/10.1017/CBO9780511808098.031

Schwenk, C. H. (1984). Cognitive Simplification Processes in Strategic Decision-Making. *Strategic Management Journal*, *5*(2), 111-128. http://www.jstor.org/stable/2486171

Schwenk, C. H. (1986). Information, cognitive biases, and commitment to a course of action. *Academy of Management Review*, *11*(2), 298-310.

Scottish Government. (2021). *Scottish Crime and Justice Survey 2019/20: main findings* (9781800). http://www.gov.scot/publications/scottish-crime-justice-survey-2019-20-main-findings/

Scroxton, A. (2023). *Russian DDoS hacktivists seen targeting western hospitals*. ComputerWeekly. Retrieved Aug 21, 2023 from https://www.computerweekly.com/news/365529957/Russian-DDoS-hacktivists-seen-targeting-western-hospitals

SecAlliance. (2022). *"The Changing Landscape of Hacktivism"*. Retrieved Jul 2, 2023 from https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: insights and implications. *Healthcare*, *8*(2), 133.

Sentinel Labs. (2022). Retrieved Jul 5, 2023 from https://www.sentinelone.com/labs/hacktivism-and-state-sponsored-knock-offs-attributing-deceptive-hack-and-leak-operations

Shahid, N., & Khan, A. (2022). Adressing Cyber-Vulnerabilities through Deterrence. *Journal of Contemporary Studies*, *11*(1), 50-68. https://doi.org/10.54690/JCS.V11I1.212

Sharma, K., Zhan, X., Nah, F. F.-H., Siau, K., & Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 69-91. https://doi.org/10.1108/OCJ-03-2021-0009

Sharma, S., & Hill, M. (2023). *The biggest data breach fines, penalties, and settlements so far*. CSO Online. Retrieved Oct 13, 2023 from https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Sharwood, S. (2022). *Belgium says Chinese cyber gangs attacked its government and military*. The Register. Retrieved Dec 9, 2023 from https://www.theregister.com/2022/07/20/belgium_alleges_china_apt_attacks/

Shayo, C., & Lin, F. (2019). An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. *Journal of Computer Science and Technology*, *7*. https://doi.org/10.15640/jcsit.v7n1a1

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice*, *124*, 523-536. https://doi.org/10.1016/J.TRA.2018.06.033

Shelly, L. (2018). *A Tangled Web: Organized Crime and Oligarchy in Putin's Russia*. Retrieved Aug 27, 2023 from https://warontherocks.com/2018/11/a-tangled-web-organized-crime-and-oligarchy-in-putins-russia/

Shepherd, D. A., Williams, T. A., & Patzelt, H. (2014). Thinking About Entrepreneurial Decision Making: Review and Research Agenda. *Journal of Management*, *41*(1), 11-46. https://doi.org/10.1177/0149206314541153

Shleifer, A. (2012). Psychologists at the Gate: A Review of Daniel Kahneman's Thinking, Fast and Slow *Journal of Economic Literature*, *50*(4), 1-12. https://doi.org/10.1257/jel.50.4.1

Simon, H. A. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, *69*(1), 99-118. https://doi.org/10.2307/1884852

Simon, H. A. (1956). Rational Choice and the Structure of the Environment. *Psychological Review*, *63*(2), 129-138.

Simpson, K. R., & Lyndon, A. (2019). False Alarms and Overmonitoring: Major Factors in Alarm Fatigue Among Labor Nurses. *Journal of Nursing Care Quality*, *34*(1).

Singh, M. M., & Bakar, A. A. (2019). A Systemic Cybercrime Stakeholders Architectural Model. *Procedia Computer Science*, *161*, 1147-1155. https://doi.org/10.1016/J.PROCS.2019.11.227

Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security*, *8*(5), 197-209.

Sloman, S. A. (1996). The empirical case for two systems of reasoning. *Psychological Bulletin*, *119*(1), 3-22. https://doi.org/10.1037/0033-2909.119.1.3

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, *177*(3), 1333-1352. https://doi.org/10.1016/j.ejor.2005.04.006

SmartPLS GmbH. (2024). *SmartPLS 4 [Computer software]*. https://www.smartpls.com

Smith, A. (2006). *Crime statistics: An independent review. Carried out for the Secretary of State for the Home Department*. http://webarchive.nationalarchives.gov.uk/20110218135832/http:/rds.homeoffice.gov.uk/rds/pdfs06/crime-statistics-independent-review-06.pdf

Smith, I. (2022). *Cyber attacks set to become 'uninsurable', says Zurich chief*. Financial Times. Retrieved Dec 2, 2023 from https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d

SOC Radar. (2023). *APT Profile: Cozy Bear/APT29*. Retrieved Jul 18, 2023 from https://socradar.io/apt-profile-cozy-bear-apt29

Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business*, *5*(7), 329-354.

Sophos. (2021). *Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year, Sophos Survey Shows*. Retrieved Aug 22, 2023 from https://www.sophos.com/en-us/press/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year

Stanovich, K., & West, R. (2008). On the Relative Independence of Thinking Biases and Cognitive Ability. *Journal of Personality and Social Psychology*, *94*, 672-695. https://doi.org/10.1037/0022-3514.94.4.672

Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*, *23*(5), 645-665. https://doi.org/10.1017/S0140525X00003435

Stanton, J., Mastrangelo, P., Stam, K., & Jolton, J. (2004). *Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices*.

Stech, K. (2016). *Peak Hosting Files for Bankruptcy Amid Videogame Dispute*. The Wall Street Journal. Retrieved Dec 1, 2023 from https://www.wsj.com/articles/peak-hosting-files-for-bankruptcy-amid-videogame-dispute-1466041447

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication (includes Communication Reports)*, *63*(3), 382-412. https://doi.org/10.1080/10570319909374648

Sudeep, S. (2021). *Nudging Our Way to Successful Information Security Awareness*. Retrieved Oct 4, 2023 from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-1/nudging-our-way-to-successful-information-security-awareness

Sullivan, J. P. (2023). The Information Age: Transnational Organized Crime, Networks, and Illicit Markets. *Journal of Strategic Security*, *16*(1), 51-71.

Sunstein, C. R., & Thaler, R. H. (2003). Libertarian paternalism is not an oxymoron. *The University of Chicago Law Review*, *70*(4), 1159-1202.

Suri, G., Sheppes, G., Schwartz, C., & Gross, J. J. (2013). Patient Inertia and the Status Quo Bias: When an Inferior Option Is Preferred. *Psychological Science*, *24*(9), 1763-1769. https://doi.org/10.1177/0956797613479976

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review*, *5*, 1-12. https://doi.org/10.2307/2083937

Sviatun, O. V., Goncharuk, O. V., Chernysh, R., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762. https://doi.org/10.37394/23207.2021.18.72

Swabey, P. (2022). *Cloudflare outage disrupts sites including Google, AWS and Twitter*. Tech Monitor. Retrieved Oct 29, 2023 from https://techmonitor.ai/technology/cloud/cloudflare-outage-disrupts-sites-google-aws-twitter

Tamm, T., Seddon, P., Parkes, A., & Kurnia, S. (2014). *A Model of Strategic IT Decision-Making Processes*.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, *33*(5), 890-911. https://doi.org/10.1080/07418825.2014.994658

Tenebruso, J. (2020). *If You Bought $10,000 of Zoom Stock at the Beginning of 2020, Here's How Much You'd Have Today* Nasdaq. Retrieved Oct 15, 2023 from https://www.nasdaq.com/articles/if-you-bought-%2410000-of-zoom-stock-at-the-beginning-of-2020-heres-how-much-youd-have-today

Thaler, R., & Mullainathan, S. (2001). Behavioral Economics. In N. S. P. Baltes (Ed.), *International Encyclopedia of the Social and Behavioral Sciences.* (pp. 1094-1100).

Thaler, R. H. (1980). Toward a positive theory of consumer choice. *Journal of Economic Behavior & Organization*, *1*(1), 39-60. https://doi.org/10.1016/0167-2681(80)90051-7

Thaler, R. H. (1999). Mental accounting matters. *Journal of Behavioral decision making*, *12*(3), 183-206.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving Decisions About Health, Wealth and Happiness*. Penguin Books.

The Decision Lab. (n. d.). *System 1 and System 2 Thinking*. Retrieved Sep 24, 2023 from https://thedecisionlab.com/reference-guide/philosophy/system-1-and-system-2-thinking

Thielman, S., & Johnston, C. (2016). *Major cyber attack disrupts internet service across Europe and US*. The Guardian. Retrieved Oct 28, 2023 from https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service

Thomas, A., & Millar, P. (2011). Reducing the Framing Effect in Older and Younger Adults by Encouraging Analytic Processing. *The journals of gerontology. Series B, Psychological sciences and social sciences*, *67*, 139-149. https://doi.org/10.1093/geronb/gbr076

Tibshirani, R. J., & Efron, B. (1993). An introduction to the bootstrap. *Monographs on statistics and applied probability*, *57*(1), 1-436.

Tidy, J. (2023a). *British Airways fined £20m over data breach*. BBC. Retrieved Oct 9, 2023 from https://www.bbc.com/news/technology-54568784

Tidy, J. (2023b). *Lapsus$: Court finds teenagers carried out hacking spree*. BBC. Retrieved Dec 11, 2023 from https://www.bbc.com/news/technology-66549159

Ting, D. (2019). *Why Cognitive Biases and Heuristics Lead to an Under-investment in Cybersecurity*.

Toet, A., Brouwer, A.-M., Bosch, K., & Korteling, J. E. (2016). Effects of personal characteristics on susceptibility to decision bias: a literature study. *International Journal of Humanities and Social Sciences*, *8*, 1-17.

Topalli, V., & Nikolovska, M. (2020). The Future of Crime: How Crime Exponentiation Will Change Our Field. *The Criminologist*, *45*(3), 1-8.

Topor, L., & Shuker, P. (2020). *Coronavirus Conspiracies and Dis/Misinformation on the Dark Web*. Retrieved Aug 11, 2023 from https://www.e-ir.info/2020/10/09/coronavirus-conspiracies-and-dis-misinformation-on-the-dark-web/

Tor. (n. d.). *Onion Services*. Retrieved Jul 5, 2023 from https://metrics.torproject.org/hidserv-dir-v3-onions-seen.html?start=2019-04-06&end=2023-07-05

Transforma Insights. (2022). *Global IoT connections to hit 29.4 billion in 2030 - Transforma Insights*. Retrieved Jun 22, 2023 from https://transformainsights.com/news/global-iot-connections-294

Trevis Certo, S., Connelly, B. L., & Tihanyi, L. (2008). Managers and their not-so rational decisions. *Business Horizons*, *51*(2), 113-119.

Trinczek, R. (2009). How to Interview Managers? Methodical and Methodological Aspects of Expert Interviews as a Qualitative Method. In A. Bogner, B. Littig, & W. Menz (Eds.), *Empirical Social Research* (pp. 203-216). Palgrave Macmillan. https://doi.org/10.1057/9780230244276_10

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573-586. https://doi.org/10.3390/jcp2030029

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229-244. https://doi.org/10.1093/JCSL/KRS019

Tsvetanov, T., & Slaria, S. (2021). The effect of the Colonial Pipeline shutdown on gasoline prices. *Economics Letters*, *209*, 110122-110122. https://doi.org/10.1016/J.ECONLET.2021.110122

Tversky, A., & Kahneman, D. (1974). Judgment Under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124-1131.

Tversky, A., & Kahneman, D. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263-291. https://doi.org/10.2307/1914185

Tversky, A., & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, *211*(4481), 453-458. https://doi.org/10.1126/SCIENCE.7455683

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, *5*(4), 297-323. https://doi.org/10.1007/BF00122574

Tzagkarakis, S. I., & Kritas, D. (2023). Mixed research methods in political science and governance: approaches and applications. *Quality & Quantity*, *57*(1), 39-53. https://doi.org/10.1007/s11135-022-01384-y

U.S. Cyber Command. (2022). *Iranian intel cyber suite of malware uses open source tools*. Retrieved Jul 2, 2023 from https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools

U.S. Department of Defense. (2021). *In Cyber, Differentiating Between State Actors, Criminals Is a Blur*. Retrieved Jun 25, 2023 from https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur

U.S. Department of Health and Human Services. (2022). Retrieved Jun 25, 2023 from https://www.hhs.gov/sites/default/files/iranian-threat-actors-and-healthcare.pdf

U.S. Department of Justice. (2014). *Dozens Of Online "Dark Markets" Seized Pursuant To Forfeiture Complaint Filed In Manhattan Federal Court In Conjunction With The Arrest Of The Operator Of Silk Road 2.0*. Retrieved Aug 25, 2023 from https://www.justice.gov/usao-sdny/pr/dozens-online-dark-markets-seized-pursuant-forfeiture-complaint-filed-manhattan-federal

U.S. Department of Justice. (2016). *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector* https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

U.S. Department of Justice. (2018a). *Jury Convicts Man Who Hacked Boston Children's Hospital And Wayside Youth & Family Support Network*. Retrieved Aug 22, 2023 from https://www.justice.gov/usao-ma/pr/jury-convicts-man-who-hacked-boston-childrens-hospital-and-wayside-youth-family-support

U.S. Department of Justice. (2018b). *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. Retrieved Aug 19, 2023 from https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

U.S. Department of Justice. (2024). *911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation*. Retrieved Aug 27, 2024 from https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation

U.S. Department of the Treasury. (2020a). *Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group* https://home.treasury.gov/news/press-releases/sm924

U.S. Department of the Treasury. (2020b). *Treasury Takes Robust Actions to Counter Ransomware*. Retrieved Aug 22, 2023 from https://home.treasury.gov/news/press-releases/jy0364

U.S. Department of the Treasury. (2021). *Ransomware Trends in Bank Secrecy Act Data between July 2021 and December 2021*. Retrieved Aug 22, 2023 from https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf

U.S. Department of the Treasury. (2022). *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*. Retrieved Jun 25, 2023 from https://home.treasury.gov/news/press-releases/jy0701

U.S. Director of National Intelligence. (2021). *The 2021 Annual Threat Assessment Report supports the Office of the Director of National Intelligence*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

U.S. White House. (2021a). *Executive Order on Improving the Nation's Cybersecurity*. Retrieved Oct 13, 2023 from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

U.S. White House. (2021b). *Fact Sheet: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident*. Retrieved Aug 27, 2023 from https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/

UNDOC. (2013). *Draft - Comprehensive Study on Cybercrime*. https://www.unodc.org/e4j/data/_university_uni_/draft_comprehensive_study_on_cybercrime.html?lng=en

UNDOC. (n. d.-a). United Nations Office on Drugs and Crime. Retrieved Jun 24, 2023 from https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/references.html

UNDOC. (n. d.-b). *Criminal groups engaging in cyber organized crime*. United Nations Office on Drugs and Crime. Retrieved Jul 10, 2023 from https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html

United Nations. (2022). *Review of Maritime Transport 2022*. https://unctad.org/publication/review-maritime-transport-2022

United Nations Security Council. (2019). *Note by the President of the Security Council*. Retrieved Jul 9, 2023 from https://daccess-ods.un.org/tmp/8394677.04296112.html

Vagle, J. L. (2020a). Cybersecurity and Moral Hazard. *Stanford Technology Law Review*, *23*.

Vagle, J. L. (2020b). *Zoom and the Problem of Cybersecurity Moral Hazard*. Retrieved Oct 14, 2023 from https://www.justsecurity.org/69863/zoom-and-the-problem-of-cybersecurity-moral-hazard/

Van Bavel, R., & Rodriguez, P. N. (2016). *Nudging Online Security Behaviour with Warning Messages: Results from an online experiment* (978-92-79-63487-1). https://publications.jrc.ec.europa.eu/repository/handle/JRC103223

Van Koppen, P. J., & Jansen, R. W. J. (1998). The road to the robbery: Travel patterns in commercial robberies. *British Journal of Criminology*, *38*(2), 230-246. https://doi.org/10.1093/OXFORDJOURNALS.BJC.A014233

van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, *90*, 101651. https://doi.org/10.1016/j.cose.2019.101651

Vanderford, R. (2023). *Merck's Insurers On the Hook in $1.4 Billion NotPetya Attack, Court Says*. The Wall Street Journal. Retrieved Aug 22, 2023 from https://www.wsj.com/articles/mercks-insurers-on-the-hook-in-1-4-billion-notpetya-attack-court-says-528aeb01

Vecchio, D. (2016). *How to Derive Business Value From DevOps*. Gartner. https://www.gartner.com/document/3510017

VERBI Software GmbH. (2023). *MAXQDA Version 24.0.0 [Computer Software]*. https://www.maxqda.com

Verizon. (2023). *2023 Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/

Verstraete, M., & Zarsky, T. (2022). Cybersecurity Spillovers. *Brigham Young University Law Review*, *47*(3).

Violino, B. (2022). *Rising premiums, more restricted cyber insurance coverage poses big risk for companies*. CNBC. Retrieved Dec 2, 2023 from https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html

Wadhwani, S. (2020). *DDoS Attacks Plague Miami-Dade County Public Schools*. Retrieved Jul 7, 2023 from https://www.spiceworks.com/it-security/network-security/news/ddos-attacks-plague-miami-dade-county-public-schools

Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature*, *533*(7602), 164-167. https://doi.org/10.1038/533164a

Wall, D. S. (2008). Cybercrime: The Transformation of Crime in the Information Age. *The British Journal of Sociology*. https://www.academia.edu/61708996/Cybercrime_The_Transformation_of_Crime_in_the_Information_Age_By_D_S_Wall

Wang, L. (2023). *Big Tech's Dominance in Stock Market Hits Breakpoint for Nasdaq 100*. Bloomberg. Retrieved Nov 24, 2023 from https://www.bloomberg.com/news/articles/2023-07-10/big-tech-s-dominance-in-stock-market-hits-breaking-point-for-nasdaq-100#xj4y7vzkg

Wang, M., Rieger, M. O., & Hens, T. (2017). The impact of culture on loss aversion. *Journal of Behavioral decision making*, *30*(2), 270-281.

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*, 101173. https://doi.org/https://doi.org/10.1016/j.pacfin.2019.101173

Wang, S. S., & Franke, U. (2020). Enterprise IT service downtime cost and risk transfer in a supply chain. *Operations Management Research*, *13*(1), 94-108. https://doi.org/10.1007/s12063-020-00148-x

Wang, Y., Arief, B., & Hernandez-Castro, J. (2023). Dark Ending: What Happens when a Dark Web Market Closes down. 106-117. https://doi.org/10.5220/0011681600003405

Ward, J., Daniel, E., & Peppard, J. (2008). Building Better Business Cases for IT Investments. *MIS Quarterly Executive*, *7*.

Wash, R., & Rader, E. (2015). Too much knowledge? security beliefs and protective behaviors among united states internet users. Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), Jul 22-24, Ottawa, Canada.

Weber, D. M., & Kauffman, R. J. (2011). What drives global ICT adoption? Analysis and research directions. *Electronic Commerce Research and Applications*, *10*(6), 683-701. https://doi.org/10.1016/J.ELERAP.2011.01.001

WEF. (2020). *Partnership against Cybercrime*. http://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf

WEF. (2023a). *Global Cybersecurity Outlook 2023*. https://www.weforum.org/reports/global-cybersecurity-outlook-2023

WEF. (2023b). *The Global Risks Report 2023*. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Weimann, G. (2004). *Cyberterrorism. How Real Is the Threat?* https://www.usip.org/sites/default/files/sr119.pdf

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, *39*(3), 195-206. https://doi.org/10.1080/1057610X.2015.1119546

Weimann, G. (2018). *Going darker? The challenge of dark net terrorism*.

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, *39*(5), 806-820. https://doi.org/10.1037/0022-3514.39.5.806

Weiser, B. (2015). *Ross Ulbricht, Creator of Silk Road Website, Is Sentenced to Life in Prison*. The New York Times. Retrieved Jul 1, 2023 from https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html

Welburn, J. W., & Strong, A. M. (2022). Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis*, *42*(8), 1606-1622. https://doi.org/10.1111/RISA.13715

White, G. L. (2015). Education and Prevention Relationships on Security Incidents for Home Computers. *The Journal of computer information systems*, *55*(3), 29-37.

Willett, M. (2023). Lessons of the SolarWinds hack. In *Survival April–May 2021: Facing Russia* (pp. 7-25). Routledge.

Williams, K. (2024). *The CrowdStrike fail and next global IT meltdown already in the making*. CNBC. Retrieved Aug 14, 2024 from https://www.cnbc.com/2024/07/20/the-crowdstrike-fail-and-next-global-it-meltdown-already-in-the-making.html

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior*, *40*(9), 1119-1131. https://doi.org/10.1080/01639625.2018.1461786

Wilson, C. (2008). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*.

Wilson, C., Gaidosch, T., Adelmann, F., & Morozova, A. (2019). *Cybersecurity Risk Supervision*. https://www.imf.org/-/media/Files/Publications/DP/2019/English/CRSEA.ashx

Wolff, J. (2022). *Insurers must rethink handling of cyber attacks on states*. Financial Times. Retrieved Dec 4, 2023 from https://www.ft.com/content/aa147054-ec14-4a75-a183-bee345319948

Wong, J. C. (2017). *Uber concealed massive hack that exposed data of 57m users and drivers.* The Guardian. Retrieved Nov 29, 2023 from https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

Woolf, N. (2016). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian. Retrieved Oct 26, 2023 from https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

World Bank. (n. d.). *GDP (current US$)*. Retrieved Nov 21, 2023 from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

Wrede, D., Stegen, T., & Graf von der Schulenburg, J. M. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *Geneva Papers on Risk and Insurance: Issues and Practice*, *45*(4), 657-689. https://doi.org/10.1057/S41288-020-00183-6/TABLES/3

Wright, G., & Goodwin, P. (2002). Eliminating a Framing Bias by Using Simple Instructions to 'Think Harder' and Respondents with Managerial Experience: Comment on

'Breaking the Frame'. *Strategic Management Journal*, *23*(11), 1059-1067. http://www.jstor.org.wwwproxy1.library.unsw.edu.au/stable/3094349

Xu, C., Guo, S., Haislip, J., & Pinsker, R. (2019). Earnings Management in Firms with Data Security Breaches. *Journal of Information Systems*, *33*. https://doi.org/10.2308/isys-52480

Yadron, D. (2015). *Iranian Hackers Infiltrated New York Dam in 2013*. The Wall Street Journal. Retrieved Aug 27, 2023 from https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

Yang, Y. (2023). *Belgium's cyber security agency links China to spear phishing attack on MP*. Financial Times. Retrieved Dec 8, 2023 from https://www.ft.com/content/5c32261c-b1a6-488e-9002-0ca9e0c8ff1b

Yunos, Z., Ahmad, R., & Yusoff, M. (2014). Grounding the component of cyber terrorism framework using the grounded theory. Proceedings of 2014 Science and Information Conference, SAI 2014, Aug 27-29, London, United Kingdom.

Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A., & Ziefle, M. (2017). Online Privacy Perceptions of Older Adults. In J. Zhou & G. Salvendy, *Human Aspects of IT for the Aged Population. Applications, Services and Contexts* Cham.

Zhang, T. (2020). *Dissertation: "Three Essays on the Economics of Cybersecurity"*. O. S. University. https://shareok.org/bitstream/handle/11244/325452/Zhang_okstate_0664D_16681.pdf?sequence=1

Zimmermann, V., & Renaud, K. (2021). The Nudge Puzzle. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *28*(1). https://doi.org/10.1145/3429888

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

LIST OF TABLES

LIST OF FIGURES

APPENDIX 1: CODEBOOK

Category	Code	Description
Uncertainty	UNC	Lack of clear understanding or predictability in cyber-threats or cyber-security measures.
Optimism Bias	OPT	Overestimating the likelihood of positive outcomes or underestimating risks in cyber-security.
Overconfidence	OVC	Excessive belief in the organization's ability to handle cyber-threats.
Availability Heuristic	AVH	Overreliance on recent, vivid, or easily recalled examples of cyber-security incidents in decision-making.
Measurement Error	MEE	Inaccurate assessment or quantification of cyber-risks or effectiveness of measures.
Lack of Knowledge	LON	Executives lack the necessary skills and expertise.
Affect Heuristic	AFH	Emotions or feelings influencing perceptions and decision-making in cyber-security.
Organizational Barriers	ORB	Structural, cultural, or procedural obstacles within the organization affecting cyber-security (incl. lack of funding, missing incentives, and insufficient management support).
Anchoring	ANC	Over-reliance on initial information or strategies when assessing cyber-security risks.
Framing	FRM	The way cyber-security issues are presented or framed influencing decision-making.
Attribution Bias	ATB	Bias in attributing causes or responsibility for cyber-security incidents or failures.

APPENDIX 2: QUESTIONNAIRE

1. What is your age cohort?

<30 years of age	30-39 years of age	40-49 years of age	>50 years of age

2. What is your gender?

Male	Female	Other	I prefer not to disclose

3. How much professional experience within the cyber/risk/data privacy domain do you possess?

<5 years	>5 years	>10 years	>15 years

4. Which best describes your functional area of responsibility?

Information Technology	Cyber-Security	Risk & Compliance incl. Data Privacy and Protection	Other

5. Which best describes your industry?

Financial Services	Healthcare	Manufacturing	Professional Services	Public Administration	Transportation and Logistics	Utilities	Other

6. What is the size of your organization?

<500 employees	500-5000 employees	5000-9999 employees	>10000 employees

7. From the corporate board's perspective, what is the management level (hierarchy) of the CISO function in your organization? The CISO function…

reports directly to the board of directors (board -1)	has one management level in between and is two levels away from the board (board -2)	has two or more management levels in between (board -3 or more)	I don't know

8. What is the functional reporting line of the CISO inside your organization? The CISO ultimately belongs to the functional area of the…

Chief Information Officer or Chief Technology Officer	Chief Executive Officer	Chief Finance Officer	Chief Operating Officer	Chief Risk Officer or Chief Compliance Officer

9. Which maturity level best describes the degree of your pre-agreed communication plan for various cyber-incidents, encompassing internal and external communication toward customers, suppliers, business partners, and other relevant stakeholders?

Non-existent	Semi-formal (e.g., guidelines, notes, checklist, handbook, roughly defined roles and responsibilities)	Formal (e.g., mandatory templates; a "situation room" with clearly defined roles, responsibilities, and deadlines)

10. Which level best describes your organization's annual external audit practice to assess the company's cyber-security posture.

Non-existent	Semi-formal (e.g., recommendations are proposed, action may or may not be taken)	Formal (e.g., findings trigger mandatory action, implementation of measures is being tracked and reported)

11. Your organization has been materially affected by a cyber-security incident (e.g., prolonged outage, data leakage, ransomware attack, phishing attack, etc.) in the past 24 months.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

12. When evaluating the CEO's top-10 strategic priorities, how does the CEO view cyber-risk?

Neither critical nor important	Important not critical	Somewhat critical and important	Critical and important	Extremely critical and important

13. Which level best summarizes your board's knowledge about cyber-risk and the cyber-threat landscape?

Very Poor	Poor	Fair	Good	Excellent

14. When it comes to cyber-security matters, which degree best describes the perceived level of granted airtime and leadership support from the board?

Very Poor	Poor	Fair	Good	Excellent

15. If you experienced a material cyber-security incident today, how much would it affect your willingness to participate in a future cyber-security survey over the next 12 months.

It significantly increases my willingness to participate.	It somewhat increases my willingness to participate.	It does not have a significant impact on my willingness to participate.	It somewhat decreases my willingness to participate.	It significantly decreases my willingness to participate.

16. What is your personal level of understanding of the cyber-threat landscape?

Very Poor	Poor	Fair	Good	Excellent

17. We regularly conduct fire drills and simulate the response to a large-scale cyber-attack at least once every 12 months.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

18. What is the threat-level resulting from cybercrime for the average organization in your peer group across the next 12 months?

Very low	Low	Average	High	Very high

19. When looking at your peer group, what is the probability that the average organization in your industry is going to encounter a material cyber-attack over the next 12 months?

Very low	Low	Average	High	Very high

20. What is the threat-level for the average organization resulting from cyber-risks posed by third parties such as customers, suppliers, and business partners?

Very low	Low	Average	High	Very high

21. What is the probability of human error inflicting or causing a material cyber-security breach at the average organization?

Very low	Low	Average	High	Very high

22. What is the threat-level resulting from cybercrime for your organization across the next 12 months?

Very low	Low	Average	High	Very high

23. What is the probability that your organization is going to encounter a material cyber-attack over the next 12 months?

Very low	Low	Average	High	Very high

24. What is the threat-level for your organization resulting from cyber-risks posed by third parties such as customers, suppliers, and business partners?

Very low	Low	Average	High	Very high

25. What is the probability of human error inflicting or causing a material cyber-security breach at your organization?

Very low	Low	Average	High	Very high

26. When looking at your peer group across your industry, the average organization possesses the necessary resources and capabilities to effectively manage and mitigate cyber-security threats.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

27. The average organization in your industry has sufficient proficiency in implementing practices to address and mitigate cybersecurity risks.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

28. The average organization within your industry possesses sufficient levels of cybersecurity knowledge among its workforce.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

29. The typical organization within your peer group has implemented detailed plans to effectively respond to cyber-security incidents.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

30. If the average organization in your industry was hit with a significant cyber-attack (such as ransomware), it would most probably take them less than 20 days to restore the services.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

31. Your organization possesses the necessary resources and capabilities to effectively manage and mitigate cyber-security threats.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

32. Your organization is proficient in executing security practices to address and mitigate cyber-security risks.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

33. What is the extent of knowledge levels regarding cyber-security across your organization’s workforce?

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

34. You have implemented detailed plans to effectively respond to cyber-security incidents.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

35. If your organization was hit with a significant cyber-attack (such as ransomware), it would probably take you less than 20 days to restore the services.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

36. In the absence of any cyber-attacks, it is hard to justify higher investments into gaining cyber resilience.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

37. In the absence of any cyber-attacks, we might reallocate cyber-security budgets or cut the spending in one of the next budget rounds.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

38. A concrete incident (security breach or outage) will probably make additional investments available and lead to an increase of spending.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

39. Recent incidents (cyber-security breaches, threats, outages) that created headlines in the news play a crucial role in our internal meetings and in shaping the direction and dynamics of our discussions.

Strongly disagree	Disagree	Neutral	Agree	Strongly agree

APPENDIX 3: FORNELL-LARCKER CRITERION

	Attack	Availability	Comms_Plan	Optimism	Overconfidence
Attack	1.000				
Availability		0.546			
Comms_Plan			1.000		
Optimism	0.260	0.226	0.132	0.680	
Overconfidence			0.428	0.310	0.628

APPENDIX 4: ANOVA RESULTS

ONEWAY Availability Optimism Overconfidence BY Q_10: Annual Audit Practice

Descriptives

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Availability	1	13	,111572838262898	,285168003175319	,079091373659253	-,060752461381887	,283898137907683	-,4734164352600290	,5134400322880680
	2	56	-,013368363901598	,345414427289080	,046157944405874	-,105870951595524	,079134223792328	-1,3493540715718600	,5365136779514050
	3	75	-,009357580252376	,358186551519870	,041359820388020	-,091768821328361	,073053660823609	-,9546422096771930	,6558033706083350
	Total	144	,000000000000000	,346918401966883	,028909866830574	-,057145908207171	,057145908207171	-1,3493540715718600	,6558033706083350
Optimism	1	13	-,188259919899810	,610791558249052	,169403098606731	-,557357564529539	,180837724729918	-1,2072985434299200	1,0004819453309300
	2	56	-,057584047128578	,486890171861611	,065063436003344	-,187974086633923	,072805992376767	-1,2147068984676900	,9601368079404600
	3	75	,075627807971972	,525900969337104	,060725813242772	-,045371016194462	,196626632138406	-1,4015233153933600	1,0034573560455600
	Total	144	,000000000000000	,522613964648213	,043551163720684	-,086087245537421	,086087245537421	-1,4015233153933600	1,0034573560455600
Overconfidence	1	13	-,426017292221986	,544491050549096	,151014646291232	-,755049941028981	-,096984643414990	-1,3726730986472500	,3909407838613780
	2	56	-,031050974160460	,526222145182200	,070319392021608	-,171974184905402	,109872236584481	-1,1866996583290200	1,1628463650927300
	3	75	,097027724691621	,557000820150465	,064316914690543	-,031126525305101	,225181974688343	-1,0139441361578700	1,6109980688192000
	Total	144	,000000000000000	,560130022406529	,046677501867211	-,092267053759748	,092267053759748	-1,3726730986472500	1,6109980688192000

ONEWAY Availability Optimism Overconfidence BY Q_10: Annual Audit Practice

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
Availability	,919	2	141	,401
Optimism	,472	2	141	,625
Overconfidence	,365	2	141	,695

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Availability	Between Groups	,178	2	,089	,738	,480
	Within Groups	17,032	141	,121		
	Total	17,210	143			
Optimism	Between Groups	1,075	2	,538	1,996	,140
	Within Groups	37,982	141	,269		
	Total	39,057	143			
Overconfidence	Between Groups	3,119	2	1,560	5,268	,006
	Within Groups	41,746	141	,296		
	Total	44,866	143			

ONEWAY Availability Optimism Overconfidence BY Q_17: Annual Fire Drills

Descriptives

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Availability	1	16	-,026331031345715	,426118743585335	,106529685896334	-,253393681938079	,200731619246649	-1,3493540715718600	,4119546368022980
	2	40	,033588831456811	,383789800611359	,060682495633689	-,089153101466605	,156330764380226	-,8795872490116260	,6558033706083350
	3	38	,063199213797653	,291054404088127	,047215259057543	-,032467988244695	,158866415840001	-,6420876946623720	,5444237555695380
	4	34	-,097875025391285	,335519910133874	,057541189875101	-,214943456425602	,019193405643031	-,9546422096771930	,5647950656776920
	5	16	,000245248890744	,301025034677574	,075256258669393	-,160159669450662	,160650167232150	-,5360364805494900	,5898608865870200
	Total	144	,000000000000000	,346918401966883	,028909866830574	-,057145908207171	,057145908207171	-1,3493540715718600	,6558033706083350
Optimism	1	16	-,269731726990224	,708079938057156	,177019984514289	-,647040892538200	,107577438557752	-1,2147068984676900	1,0004819453309300
	2	40	-,094765497269007	,387790814210607	,061315111429836	-,218787016419160	,029256021881146	-,9137726255800860	,6441999677824530
	3	38	,051677063327827	,483410306553220	,078419506918321	-,107215950544512	,210570077200167	-1,0253498521568400	,9944361499358690
	4	34	,143354909085315	,553811726467541	,094977927524513	-,049879137383319	,336588955553950	-1,4015233153933600	,9004376574125340
	5	16	,079283262952857	,546479260009047	,136619815002262	-,211914979648172	,370481505553885	-1,0299322613145900	1,0034573560455600
	Total	144	,000000000000000	,522613964648213	,043551163720684	-,086087245537421	,086087245537421	-1,4015233153933600	1,0034573560455600
Overconfidence	1	16	-,399080470802137	,529778428291887	,132444607072972	-,681379468359663	-,116781473244611	-1,3726730986472500	,4779301234157520
	2	40	-,236961656248549	,483559034790209	,076457396654483	-,391611338231199	-,082311974265899	-1,1866996583290200	,9011201740553470
	3	38	,078080813348777	,476282377292185	,077263204103876	-,078469308475956	,234630935173510	-,8077042067954090	1,1628463650927300
	4	34	,226182850454136	,579349012355760	,099357535922723	,024038423702508	,428327277205764	-,8720365201072980	1,6109980688192000
	5	16	,325404122505123	,490387643511357	,122596910877839	,064094992527523	,586713252482723	-,8089197479095210	,9717234222614920
	Total	144	,000000000000000	,560130022406529	,046677501867211	-,092267053759748	,092267053759748	-1,3726730986472500	1,6109980688192000

ONEWAY Availability Optimism Overconfidence BY Q_17: Annual Fire Drills

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
Availability	,409	4	139	,802
Optimism	2,548	4	139	,042
Overconfidence	,386	4	139	,818

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Availability	Between Groups	,534	4	,133	1,112	,353
	Within Groups	16,677	139	,120		
	Total	17,210	143			
Optimism	Between Groups	2,424	4	,606	2,299	,062
	Within Groups	36,633	139	,264		
	Total	39,057	143			
Overconfidence	Between Groups	8,460	4	2,115	8,075	,000
	Within Groups	36,406	139	,262		
	Total	44,866	143			

ONEWAY Availability Optimism Overconfidence BY Q_8_2groups: Tech (CIO/CTO) vs. non-Tech Reporting Line

Descriptives

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Availability	0	76	-,001354123900452	,315115547381014	,036146232278220	-,073361111080944	,070652863280040	-,8795872490116260	,5788835302528790
	1	68	,001513432594623	,381723492858322	,046290772965723	-,090883336959230	,093910202148476	-1,3493540715718600	,6558033706083350
	Total	144	,000000000000000	,346918401966883	,028909866830574	-,057145908207171	,057145908207171	-1,3493540715718600	,6558033706083350
Optimism	0	76	-,021475087785379	,543498473487315	,062343550576311	-,145669809176570	,102719633605812	-1,4015233153933600	1,0004819453309300
	1	68	,024001568701306	,501168915112015	,060775658037737	-,097307152463377	,145310289865990	-1,2147068984676900	1,0034573560455600
	Total	144	,000000000000000	,522613964648213	,043551163720684	-,086087245537421	,086087245537421	-1,4015233153933600	1,0034573560455600
Overconfidence	0	76	-,076980774203781	,573884291179866	,065829042908908	-,208118952378495	,054157403970933	-1,3726730986472500	,9105604378808120
	1	68	,086037335874814	,535475023413539	,064935884747474	-,043575232557143	,215649904306770	-,8518419602310470	1,6109980688192000
	Total	144	,000000000000000	,560130022406529	,046677501867211	-,092267053759748	,092267053759748	-1,3726730986472500	1,6109980688192000

ONEWAY Availability Optimism Overconfidence BY Q_8_2groups: Tech (CIO/CTO) vs. non-Tech Reporting Line

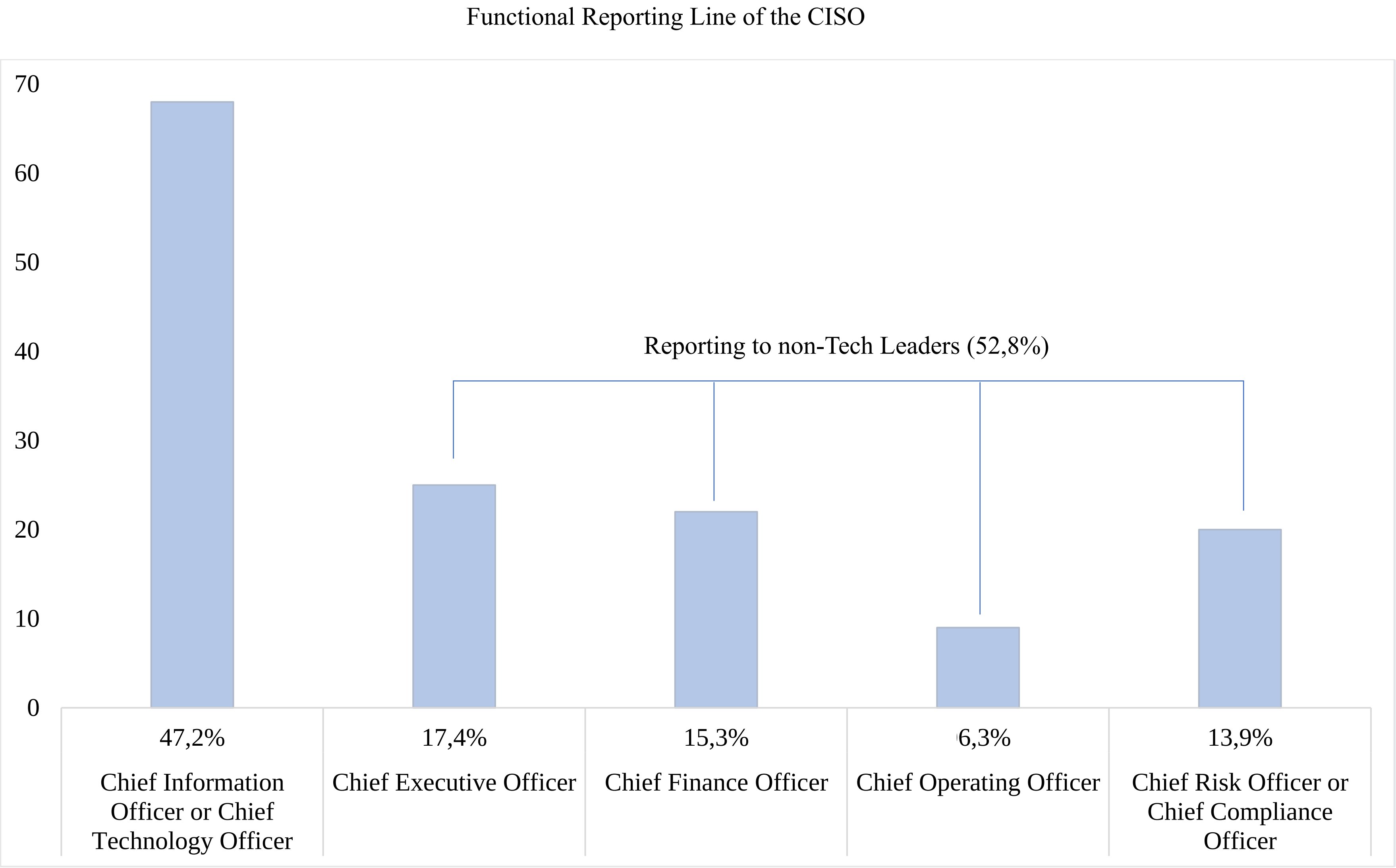
Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
Availability	1,595	1	142	,209
Optimism	,582	1	142	,447
Overconfidence	,906	1	142	,343

ANOVA

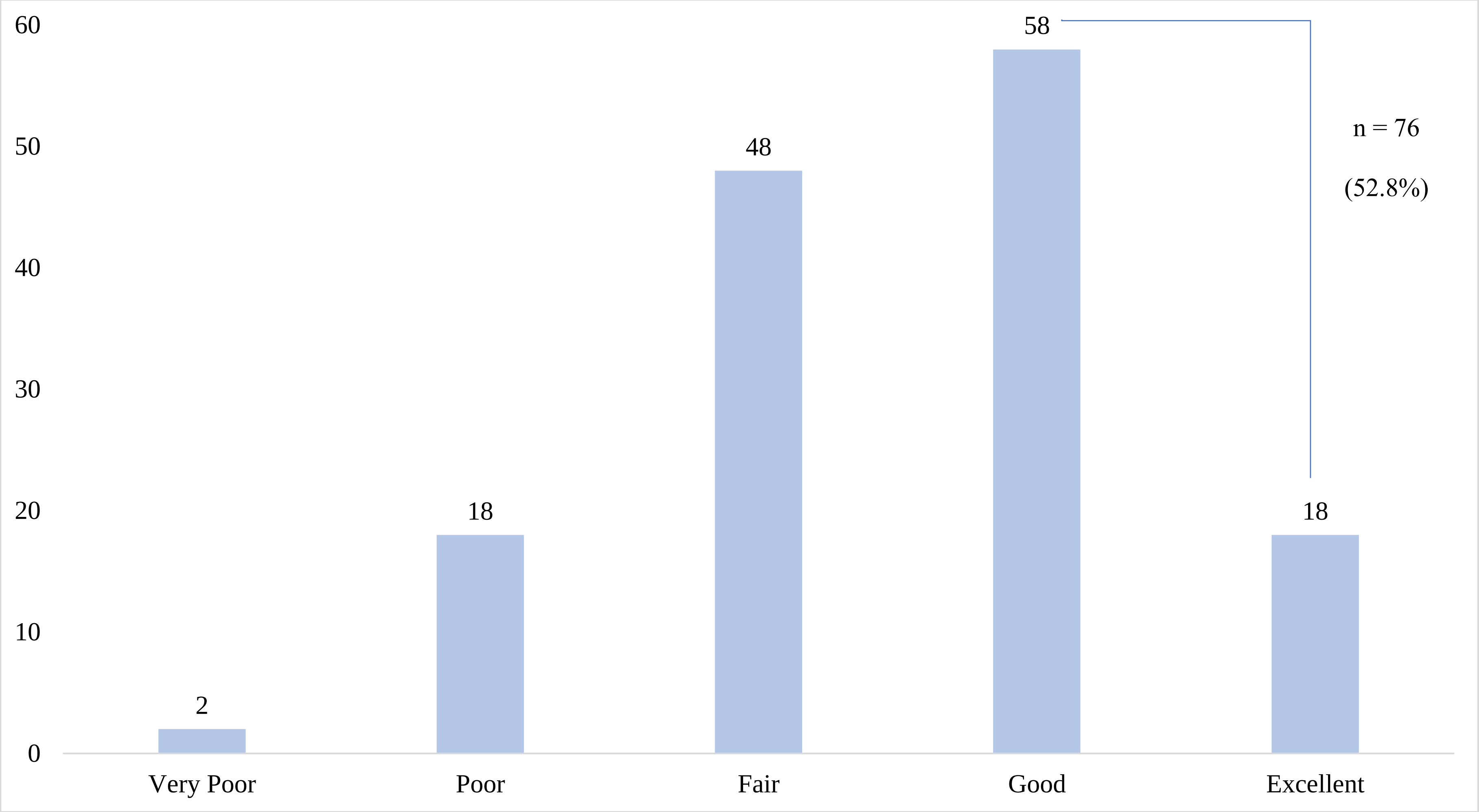
		Sum of Squares	df	Mean Square	F	Sig.
Availability	Between Groups	,000	1	,000	,002	,961
	Within Groups	17,210	142	,121		
	Total	17,210	143			
Optimism	Between Groups	,074	1	,074	,270	,604
	Within Groups	38,983	142	,275		
	Total	39,057	143			
Overconfidence	Between Groups	,954	1	,954	3,084	,081
	Within Groups	43,912	142	,309		
	Total	44,866	143			

APPENDIX 5: DISTRIBUTION OF RESPONSES TO QUESTION 8

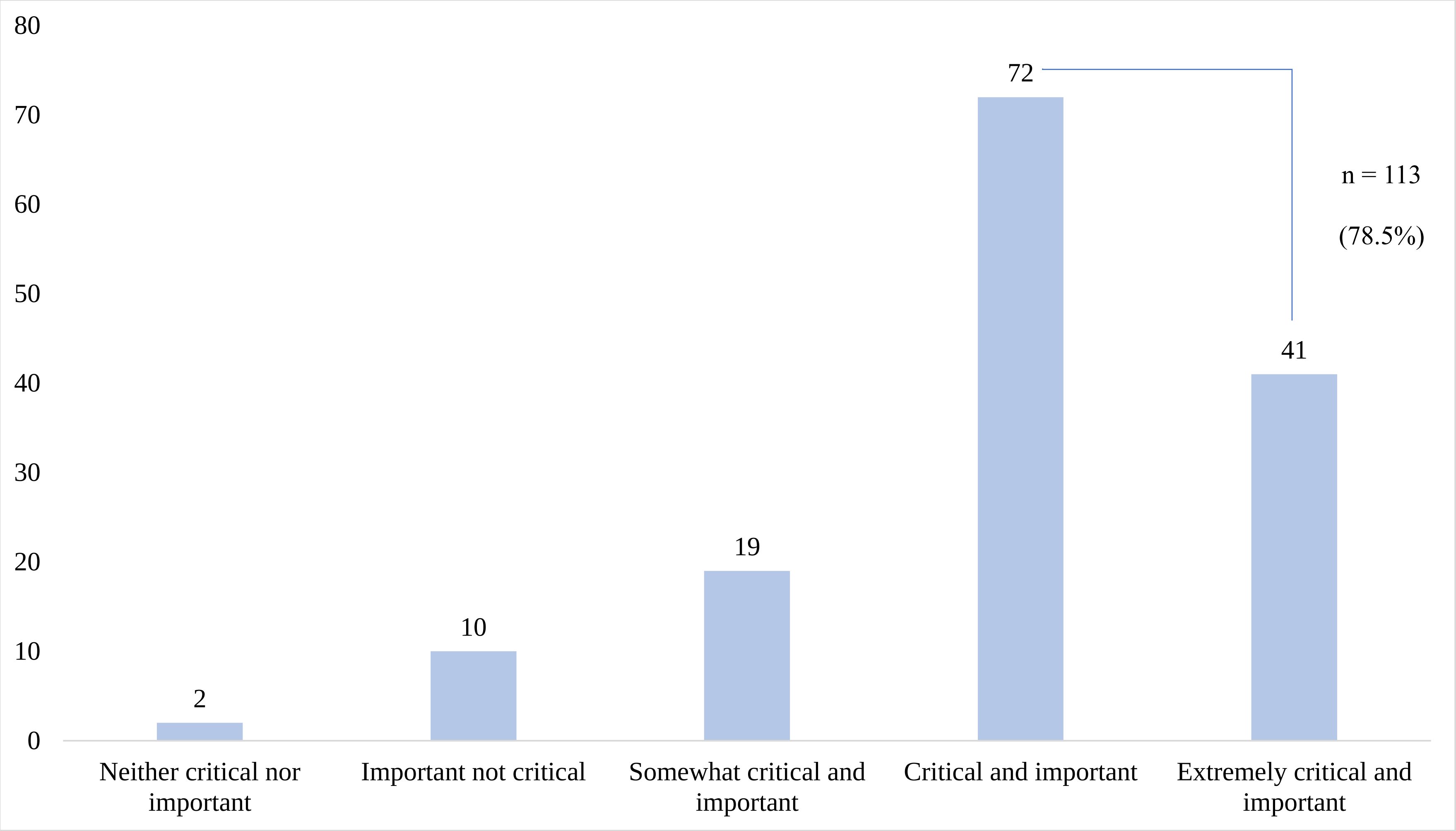


APPENDIX 6: DISTRIBUTION OF RESPONSES TO QUESTION 13

Which Level best summarizes the Board's Knowledge about Cyber-Risk and the Cyber-Threat Landscape

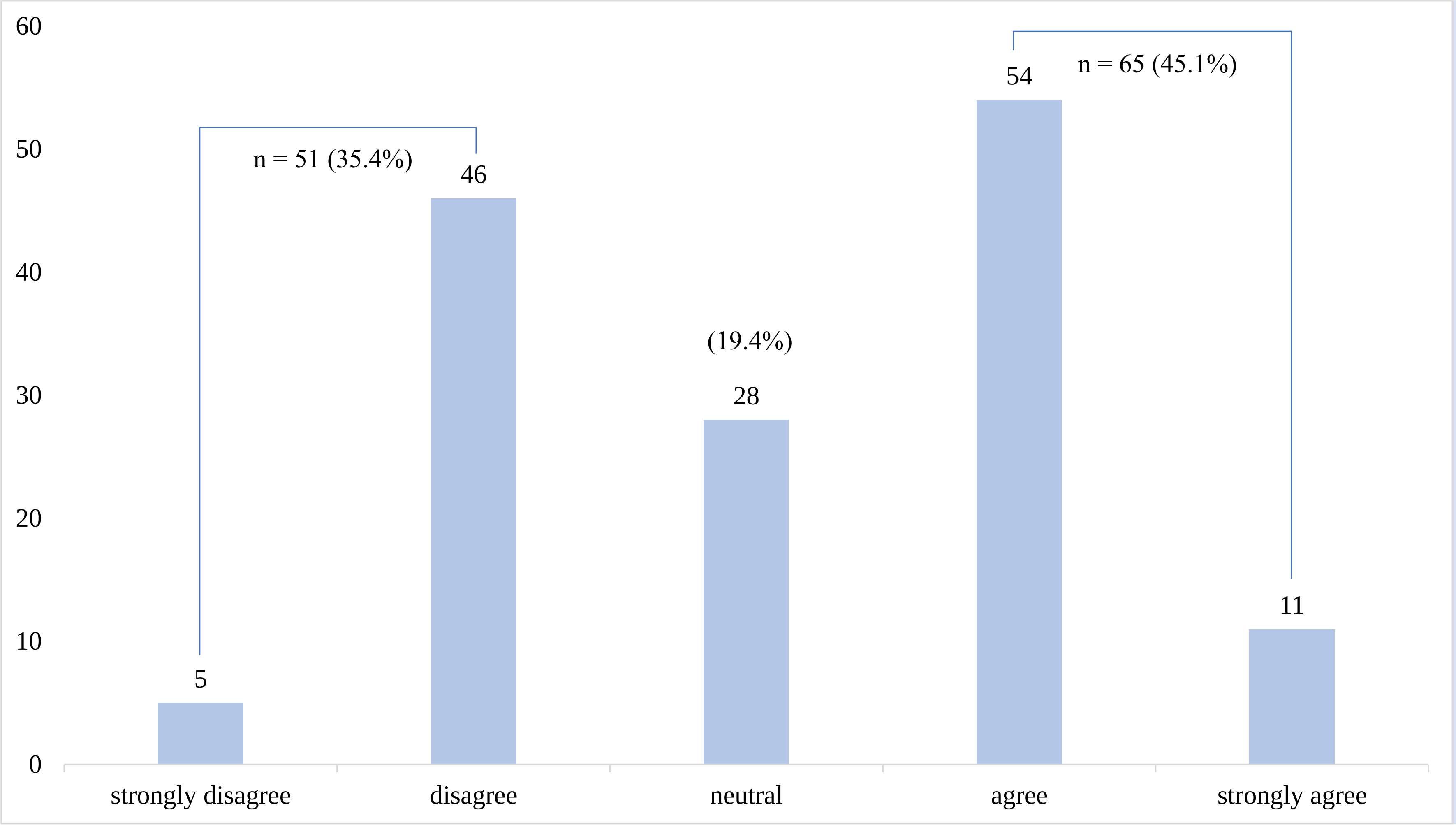


APPENDIX 7: DISTRIBUTION OF RESPONSES TO QUESTION 12



APPENDIX 8: DISTRIBUTION OF RESPONSES TO QUESTION 36

Difficulty of justifying additional Investments in Cyber-Resilience in the Absence of Attacks


n = 51 (35.4%)
n = 65 (45.1%)
(19.4%)
strongly disagree
disagree
neutral
agree
strongly agree