Commtel Whitepaper Series
August 2022

THE IMPACT OF CYBER-PHYSICAL SECURITY ON CRITICAL NATIONAL INFRASTRUCTURE

Report by Critical Future Ltd
for Commtel Networks, 2022

CRITICAL FUTURE

commtel
ENGINEERING INTELLIGENCE

EXECUTIVE SUMMARY

"More than $36 billion of economic value can be unlocked through improvements in the cyber-physical security of Critical National Infrastructure"

This report analyzes the impact of security, both cyber and physical, on Critical National Infrastructure (CNI). A key finding of the report is that an increase of $16 billion in energy investments can be achieved by implementing incremental improvements on cybersecurity.

Another important finding is that in North America, more than $12.34 billion in economic value can be added to the economy through improvements in cybersecurity systems.

For cybersecurity and physical security systems integration, there is a huge opportunity to unlock economic value. The original econometric model developed for this report finds that each **1% improvement on the overall level of cybersecurity can lead to higher growth in the transport, storage and communications industry by an estimated:**

1. $36 billion globally
2. $12.34 billion in North America
3. $2 billion in the Middle East
4. $890 million in India

These findings imply that security improvements in modern cyber-physical systems for CNI (not only in energy or transport, storage and communications) can have multiple economic benefits.

Many papers highlight the need for integration between cyber and physical security systems in CNI. This is because physical systems can be a point of entry for cyberattacks; and also, because cyberattacks can lead to physical attacks, from workplace interruptions to loss of life. **An integrated cyber-physical security solution can provide multiple benefits like:**

- Integration of many separate security systems, both cyber and physical, which will lead to better security, minimizing risks and increasing organizational resilience.
- Better management of big data generated by systems.
- Improvements to cyber-physical security overall, which will lead to better performance through its AI-based decision-making and decision-executing system.

The report also finds that there is a **negative correlation between digital and economic growth.** This happens because of many different factors, including the fact that cyberattacks on new digital systems can lead to interruptions and stall growth. **In order for a country or organization to be able to harness the power of new digital technologies, a corresponding level of security needs to be in place.**

TABLE OF CONTENTS

THE COMPLEXITIES OF MODERN CNI SECURITY

One of the biggest threats a nation can face is an attack on its Critical National Infrastructure (CNI), which includes such key services and infrastructures such as chemical, civil nuclear, communications, national security and defense, emergency services, energy, transportation, and government agencies. As years go by and nations rely more and more on IT systems and services in order to run day-to-day operations, the threat starts becoming different in nature (more complex) and in scale (more dangerous). In addition to physical threats, cyberthreats are becoming a growing area of concern. Cybersecurity needs to become a main area of government and corporate focus, to ensure the integrity and safety of public or private CNI facilities. Cybersecurity needs to be entangled with every other aspect of modern CNIs.

Such attacks are a clear and present threat to nations. Past examples include [49,19,39]:

- In 2013, the substation control house of the Arkansas electrical grid was set on fire. More than 1,000 people suffered a blackout as a result.
- In 2016, a power facility in Ukraine was the target of an intentional and potentially deadly cyberattack. The Ivano-Frankivsk region (around 700,000 individuals) in Ukraine was left without power in mid-December because of this malware attack.
- On January 21, 2016, a grand jury in the Southern District of New York indicted seven Iranian nationals for their involvement in conspiracies to conduct a coordinated campaign of distributed denial-of-service ("DDoS") attacks against the United States financial sector and other United States companies from 2011 through 2013.
- Israeli water systems were cyberattacked on a number of occasions in mid-2020. The goal of the attacks was to compromise the ICS control and command systems for Israel's wastewater plants, agriculture pumps, pumping stations and sewer systems.
- In 2021, hackers attacked the Colonial Pipeline (CP) in the US. Attackers (DarkSide RaaS) gained initial access to CP's network through a legacy VPN account that CP's IT team did not know existed. As a result, 45% of all supplies on the US East Coast were disrupted and there was a spike in gas prices.

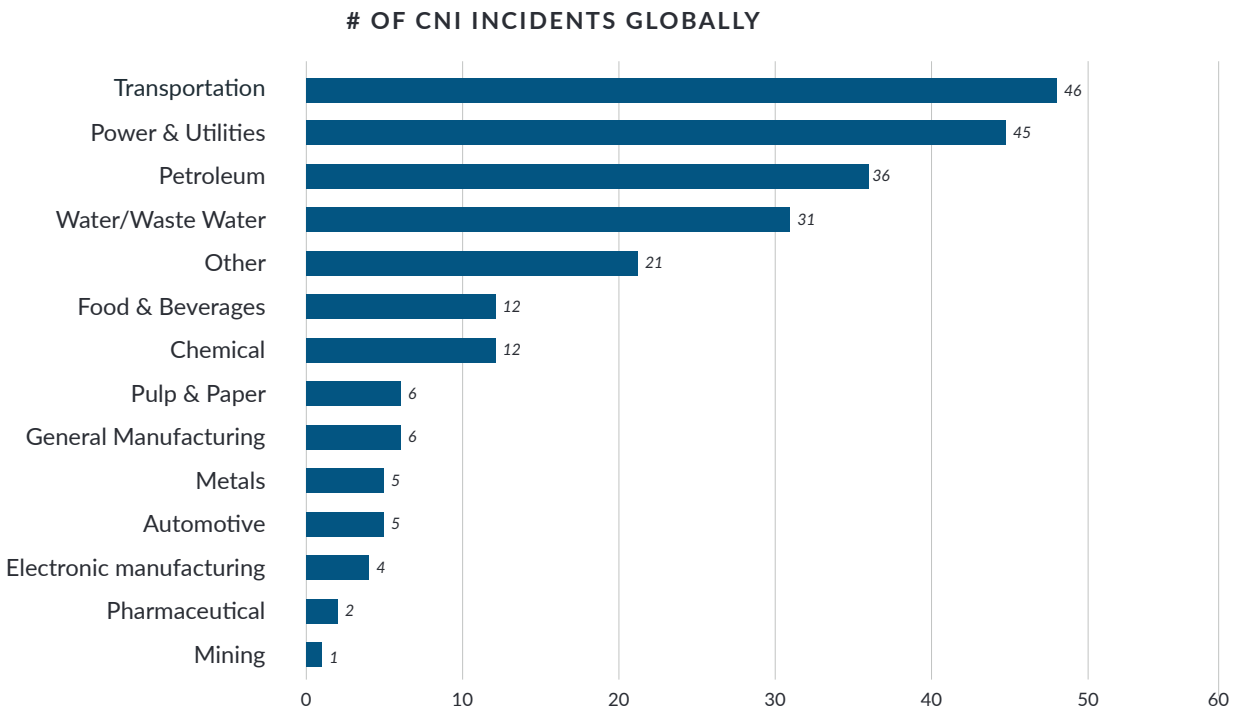

Figure 1: Number of CNI incidents globally

Source: RISI online incidents database

No specific industry can claim to be free from the threat of attack, but some are targeted more than others. According to data gathered from the Repository of Industrial Security Incidents (RISI), the industry that was targeted the most during the 1982–2014 period was transportation, followed by power and utilities, petroleum, and water/waste water. These four industries seem to have a disproportionately higher threat level than the others.

According to the UK's Centre for the Protection of National Infrastructure (CPNI):

> National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organizations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public.

From those elements within national infrastructure, not everything is considered critical. Elements are considered critical if their loss or compromise could lead to:

1. major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts
2. significant impact on national security, national defense, or the functioning of the state.

PHYSICAL SECURITY

The protection of national infrastructure from physical threats such as terrorist attacks or natural disasters, is also paramount.

According to a 2021 post from the UK Parliament:

> *Infrastructure is vital for modern society, the economy and human quality of life. Disruption to infrastructure can have widespread impacts on individuals and the economy. Two key factors that present threats to national infrastructure include climate change and malicious attacks by bad actors.*

CNIs are also in constant danger from many types of **malicious attacks.** The motivations of those attacks can be financial gain, terrorism and espionage. Most, if not all, facilities are well guarded and have gates, fences, cameras, sensors and perimeter detection systems. Overall physical security can be very well established in most of the vital infrastructures.

Climate change is increasing both the frequency and magnitude of extreme weather effects such as floods, heavy rainfall, high temperatures, droughts and strong winds. An example of this from the UK would be the 2019 extreme heatwave, which caused railway tracks to buckle and electrical wires to expand and sag. This resulted in many changes in timetables and speed restrictions, as well as one-third of the trains being canceled across the South East. Similar issues were reported in Germany, France and Australia. In more general terms, we can refer to natural disasters like floods and earthquakes as a threat to a country's CNI.

CYBERSECURITY CHALLENGES

Countries and organizations face a lot of challenges in cybersecurity capacity building (CCB), especially countries that are in a transitional stage in regard to digital transformation of their infrastructures, or organizations that are relatively young. These challenges can include institutional reform, organizational adaptation, human resource development and the support provided to increase their potential in utilizing the new systems [23,5]. Most of the issues are associated with the lack of cybersecurity culture and an inability to understand both the threat level posed and the consequences of a security breach [27].

More specifically, what is happening is that the interconnected nature of many digital technologies or critical infrastructure systems has introduced a host of new vulnerabilities. In reality, "cybersecurity is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace" [35]. With this in mind, we can define cybersecurity as "designing and implementing effective controls which will help protect enterprises and individuals from intentional attacks, breaches, incidents and consequences" [28].

In the last 15 years, according to a 2018 paper [29], numerous issues have occurred that affect the shift from information security to cybersecurity, such as:

- increased internal threats – internal "WikiLeaks" incidents, data breaches, attacks from within
- emerging technologies, namely digital technologies that are externally oriented and enable the interconnectivity of devices that constantly interact – cloud computing, sensors and Internet of Things (IoT) and cognitive technologies such as AI, mobile technology and social media
- increased external threats – malware, ransomware, data breaches, interconnected devices, IoT devices, cyberwar, state-sponsored attacks: for example, Ponemon Institute estimated that the direct cost of data breaches in 2017 was $3.62 million, while ISACA revealed that a single data breach cost – direct and indirect expenses – was around $5.5 million USD
- huge data proliferation – the volume of data transmitted over interconnected systems is doubling every 20 months, mobile internet data is doubling every year

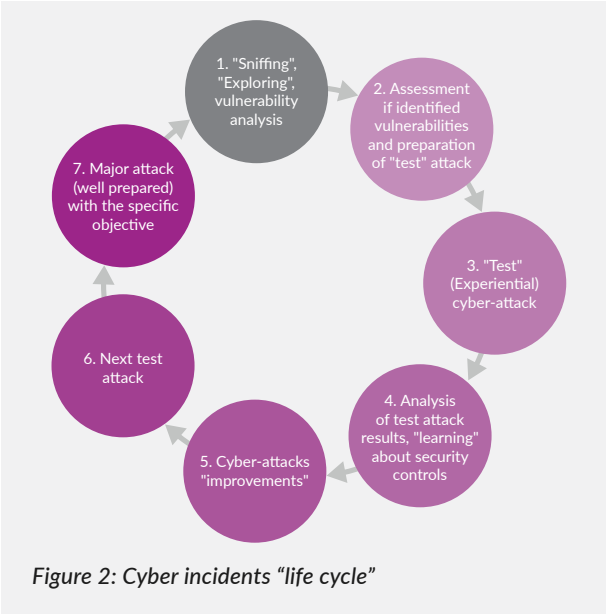

Figure 2: Cyber incidents "life cycle"

- extensive use of mobile devices and social media networks and increasingly mobile workforce – if not managed properly, bring your own device (BYOD) means "bring your own risks"
- strong regulation at international and national domain in the area of internet security and data privacy – for example, more than 60 countries have their own data protection law, the General Data Protection Regulation (GDPR), which came into effect in May 2018.

In a 2021 study[50], 73% of CIOs (Chief Information Officers) and CISOs (Chief Information Security Officers) were "highly confident" their organizations would not suffer an operational technology (OT) breach the following year, despite **83% having suffered such an incident over the past 36 months**. The belief that their infrastructure is safe can be another factor that contributes to inadequate security.

CNI security incidents can have a very negative impact in many different ways, both direct (line downtime, inability to implement processes, data breaches, etc.) and indirect (like legal obligations, lost privacy, stolen identities, regulatory penalties, loss of reputation and bad public image). According to the EY, many organizations still do not have sound policies to manage this [14].

Cyber incidents have a carefully planned "life cycle", consisting of the following phases [29]:

- "sniffing", "exploring", vulnerability analysis
- assessment of identified vulnerabilities and preparation of "test" attack
- "test" (experiential) cyberattack
- analysis of test attack results; "learning" about security controls that should detect and prevent the attack
- cyberattack "improvements"
- next test attack
- major attack (well prepared) with a specific objective.

Countries, especially developing ones, that want to build the right capabilities may face challenges on many different levels. These challenges include human resources training, organizational adaptation, institutional reforms, providing support and increasing access in order to reap the benefits of the internet and other elements of cyberspace.

Some of the main challenges that countries face include[23]:

- **Access versus institutional stability.** Access to cyberspace is increasing day by day faster than institutions have the ability, not only to fully manage but also to support the right frameworks. Excessively fast growth in access can create more damages than benefits. Without the right processes and safety measures in place, people can easily become targets for cybercrime. So the challenge is to create the structures necessary to harness the power of new technologies, at the same time guarding against malware threats that increase in line with access to cyberspace. A country needs to identify the areas that its own capabilities are lacking, and strengthen them.
- **Legal framework.** A legal framework that is able to enact decisions for building a secure cyberspace is essential. This makes it possible for governments to punish crimes and control how the digital transformation of CNIs is implemented. Something like this, however, is a challenge because the creation of such laws would also mean establishing the appropriate institutions to combat cybercrime and offer training to the stakeholders tasked

with fighting it. Also, a legislative framework that reaches too broadly is difficult to uphold and a framework that does not include enough will not be adequate. Striking the right balance is not always easy to accomplish.

- **Affordability.** Many nations do not have the necessary resources in order to achieve high standards of cybersecurity. Implementing frameworks and infrastructure is of limited use if the receiving country does not have the capacity to maintain it. It is thus imperative to create frameworks and infrastructure that a country, especially a developing one, can maintain. The local personnel need the right training in maintaining the frameworks and infrastructures implemented. This gives the country in question independence to generate and uphold its own systems.
- **Building knowledge, understanding and awareness.** Educating people about the threats and risks that follow the implementation of cyber technologies is essential. An unclear understanding of the importance of cybersecurity can render the efforts of securing a system ineffective or even useless. Governments need a good level of understanding of security challenges that arise from the use of new technologies. Implementing effective cybersecurity measures can be very difficult without this.
- **Public–private cooperation.** Much of the internet is privately owned. There is a need to strengthen the cooperation between the private and public sectors, so that stronger cybersecurity can be developed. A public–private model of this type is essential.

According to CPNI, there should be a specific "criticalities process" to collect and structure data that supports the systematic identification of the essential functions of CNI. This allows the government to build a CNI knowledge base that helps in the analysis, mapping and visualization of threats. The process goes as follows:

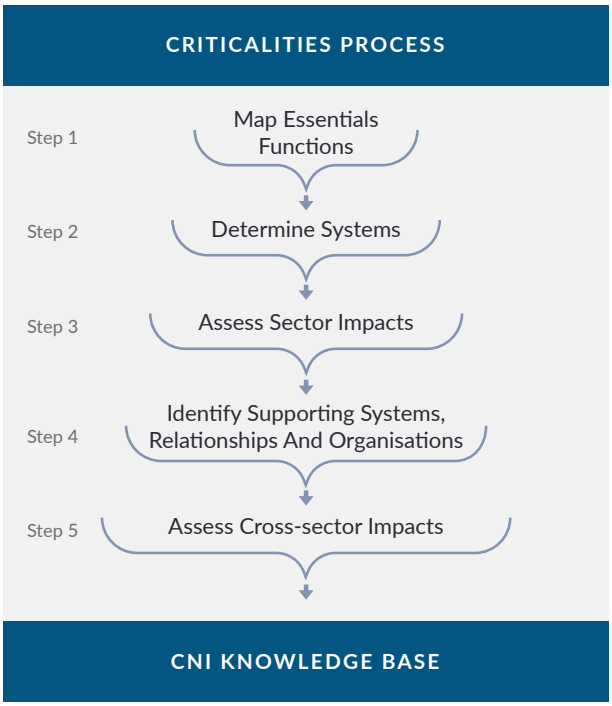

Figure 3: Criticalities process

Source: Protection of National Infrastructure In the future, building cybersecurity capabilities is going to be key for countries and organizations in order to build organizational resilience.

CYBER-PHYSICAL SECURITY

Both cyber and physical security do not exist in a vacuum. Instead, they are highly dependent on each other. A weak or subpar cyber defense system can be exploited in order for someone to gain access to the infrastructure and cause physical damage to facilities. Also, although this is a bit rarer, a breach on physical security can lead to a cyberattack.

But what is a cyber-physical system?

First of all, a cyber-physical system (CPS), according to Etesami & Basar [13], is an integration of many components, both physical and cyber (for example, digital controllers or computing devices) and the communication networks between them. Such systems have become an inseparable part of modern organizations, with applications such as smart grids, sensor networks, smart transportation systems and IoT.

Most organizations today use some type of CPS, meaning that their daily operations include interaction between physical and cyber elements. CPS applications are widely used in many CNI industries like oil and gas, the power grid, national defense and public infrastructures [2]. Therefore, the security of CPS has become a matter of utmost importance, since now a potential malicious attack is not limited to disrupting a single enterprise or isolated machine but can cause problems for the economy of a country as a whole. According to Al-Mhiqani et al. [2], an attack on a CPS can:

...provide destruction to critical infrastructure systems which are used in sectors such as defense, finance, health, and the public. To accomplish their goals criminals, activists, or terrorists are mostly looking for new and innovative techniques and targets, so cyber-physical systems are currently one of the important targets for the hackers.

Attacks against a CPS can be categorized in many different ways. Starting with the type of attack, these can be split into four different types:

1. **Worm:** A worm is a malicious self-replicating application that can spread into uninfected systems by itself without human intervention. For propagation, a worm relies on vulnerabilities of networking protocols.
2. **Trojan:** A Trojan Horse is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain access to users' systems [42].
3. **Virus**: A computer virus is a type of malicious code or program written to alter the way a computer operates, and is designed to spread from one computer to another. According to Norton, "a virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code." In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data [45].

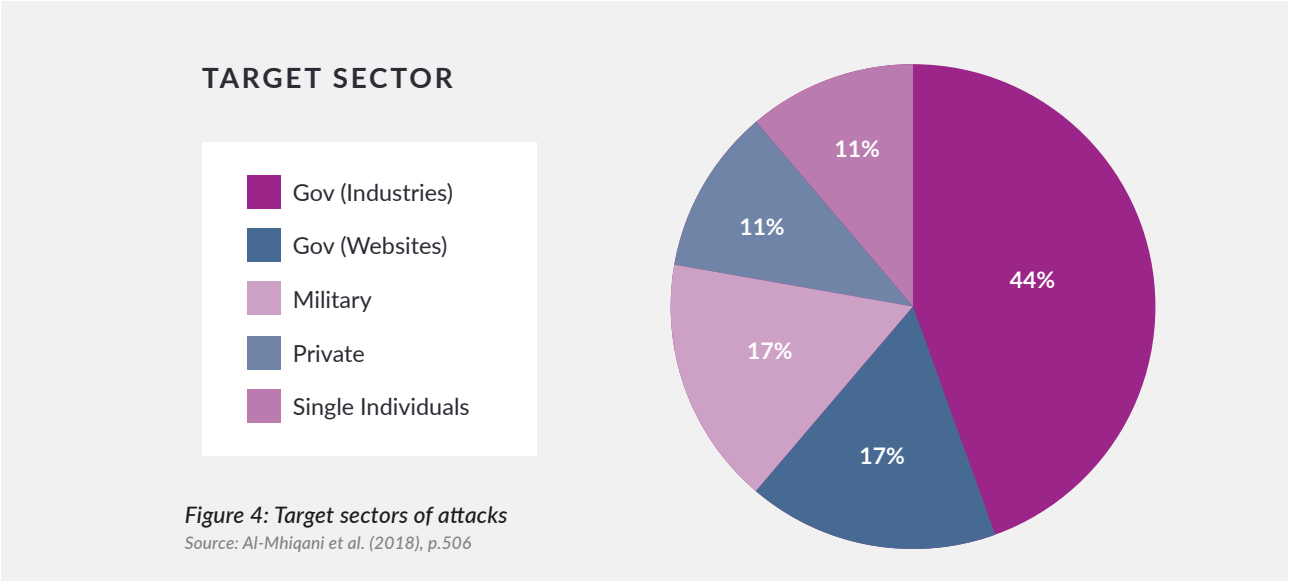

Figure 4: Target sectors of attacks
Source: Al-Mhiqani et al. (2018), p.506

4. **DDoS:** A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. DDoS attacks can be very effective because they use multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices [40].

Another useful way to categorize the attacks is **by incident type.** The attacks can be categorized as:

1. **Cyberwarfare (CW):** "the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes," according to Oxford Languages.
2. **Hacktivism (H):** the act of gaining "unauthorized access to computer files or networks in order to further social or political ends," according to Oxford Languages.
3. **Cyberespionage (CE):** the corporate arm of high-tech crime. It mainly involves attacks on companies and institutions, not individuals. Cyberespionage does not always necessarily occur on a large scale [7].
4. **Cybercrime (CC):** involves all the criminal acts that deal with networks and computers (hacking). Additionally, traditional crimes that are conducted through the internet are included in cybercrime [10].

One last way to look at attacks is by target. Usual targets of attacks are local or national governments, private organizations or companies, specific industries or utilities like electricity, gas and water.

Al-Mhiqani, et al. [2] provide the above graph on the breakdown of the targets of those attacks. As we can see, governments are by far the most common target.

CPS systems are widely used and growing, carrying associated risks to governments and organizations. As modern CNI security uses CPS systems, it should be designed to manage the security of those systems separately, as well as the security of the interactions between systems and their interconnectedness. In fact, in certain circumstances, failure of cyber-physical systems can be catastrophic in incidents such as "terrorist attacks due to failure of national defense organization, political chaos due to hacking of classified information, or information leakage of nations' nuclear infrastructures" [33].

The development of holistic solutions addressing systematic cyber-physical security in order to prevent strategic attacks, where the more traditional defensive methods have shortcomings, is a necessity.

THE COST OF CYBERCRIME

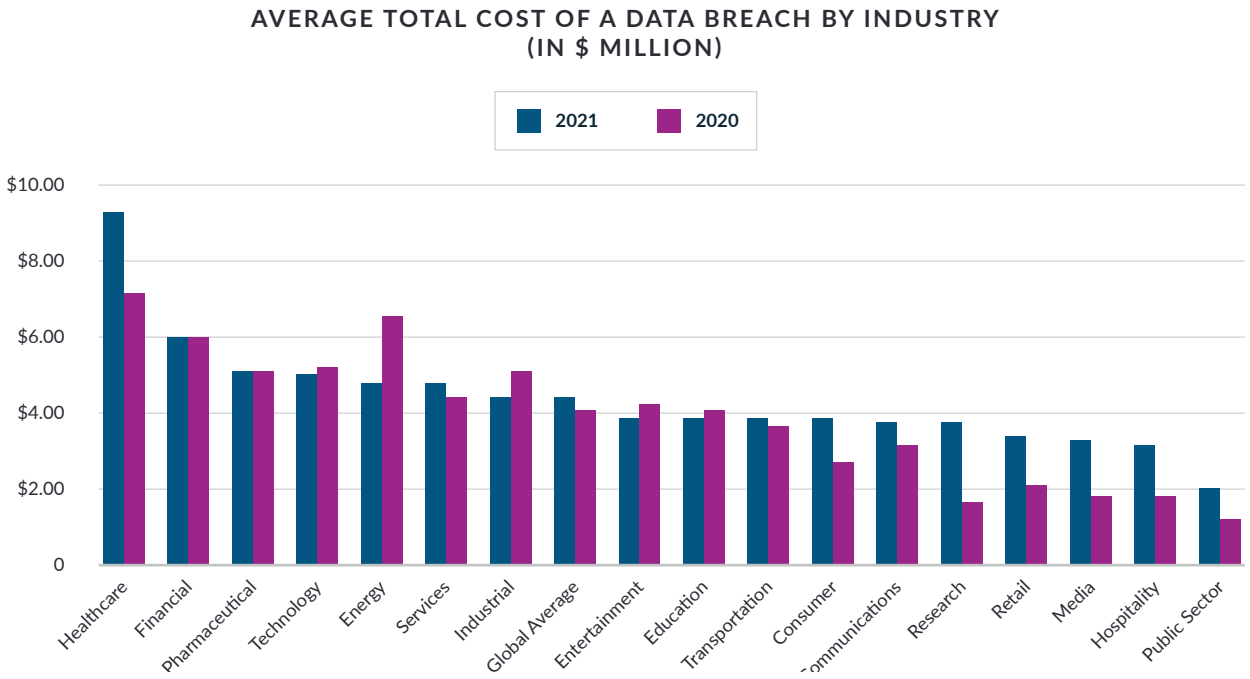

Figure 5: Cost of data breaches

Source: Cost of a data breach report, 2021

Assessing the true cost of cybercrime is a difficult task. Quantifying the true number of victims and the actual cost is challenging as attacks are so widespread and their implications so far-reaching. In this part of the report, we aim to reveal the magnitude of the problem by analyzing specific areas and presenting a series of credible statistics.

Cost of data breaches

Data breaches are a massive issue for any industry. A recent IBM report[51] estimated the average total cost of a data breach at around $4.24 million for 2021, $3.86 million higher than the previous year. The industries with the highest average cost were the healthcare, financial and pharmaceuticals industries, followed by the technology, energy and services industries, as shown in Figure 5.

An earlier 2019 report[52], made by a collaboration between Accenture and Ponemon Institute, found that the average cost of cybercrime (overall, not just data breaches) per organization was around $13 million. It is also worth noting that the report provides the growth rate of the financial consequences in each type of attack. In the last year alone, the financial consequences of ransomware have increased by 21 percent. Organizations should not overlook this fast-growing threat. Detailed analysis of their findings regarding the costs of the various types of attacks is displayed in Figure 6 overleaf.

CONSEQUENCES OF DIFFERENT TYPES OF CYBERATTACKS (AVERAGE ANNUAL COST IN US MILLION DOLLARS)

	Business disruption	Information loss	Revenue loss	Equipment damage	**Total cost by attack type**
Malware (+11%)	$0.5	$1.4	$0.6	$0.1	$2.6
Web-based attacks (+17%)	$0.3	$1.4	$0.6	–	$2.3
Denial of service (+10%)	$1.1	$0.2	$0.4	$0.1	$1.7
Malicious insiders (+15%)	$0.6	$0.6	$0.3	$0.1	$1.6
Phishing and social engineering (+8%)	$0.4	$0.7	$0.3	–	$1.4
Malicious code (+9%)	$0.2	$0.9	$0.2	–	$1.4
Stolen devices (+12%)	$0.4	$0.4	$0.1	$0.1	$1.0
Ransomware (+21%)	$0.2	$0.3	$0.1	$0.1	$0.7
Botnets (+12%)	$0.1	$0.2	$0.1	–	$0.4
Total cost by consequence	$4.0	$5.9	$2.6	$0.5	**$13.0**

Figure 6: Cost of cyberattacks
Source: The cost of cybercrime, 2019

It is estimated that around 30,000 websites are hacked every day. From 2009 to 2018 the number of malware attacks has been growing exponentially, exceeding 812 million in 2018 [46].

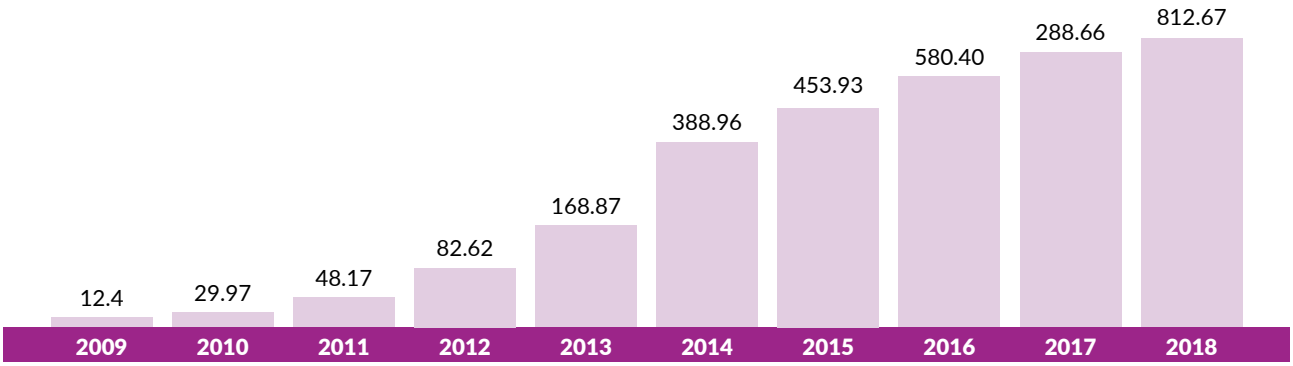

Figure 7: Malware infection growth rate (in millions)
Source: purplesec.us

Combined with previous statistics, this suggests that the **threats and potential costs for corporations are only going to increase in the future.**

ENERGY OIL AND GAS, POWER, PETROCHEMICALS

Energy is a very important sector for any country and its economy. Today, energy is becoming increasingly connected to digital technologies and ICT (information and communications technology) networks. This increasing degree of digitalization makes the energy system "smarter", allowing it to benefit from various innovative energy services, but it also makes it more vulnerable by exposing it to cyberspace, creating significant risks and potentially jeopardizing the security of energy supply and the privacy of consumer data [6].

For the purpose of this paper, energy can refer to primary energy, like oil or gas; secondary energy, like diesel, electricity or kerosene; and tertiary energy, like heating and lighting.

An energy system is a system that is responsible for "transporting and converting primary or secondary energy to meet the energy needs of an end user, such as a sector or a service (as tertiary energy) within the sector" [6]. A representation of an energy system can be found in Figure 8.

The first mission is identifying the entities critical to the energy system, as shown in Figure 8. After that, it is necessary to identify the threats that each entity may face and assess vulnerabilities. Assessing the threats should lead to actions that are going to reduce the vulnerability of the infrastructure and its likelihood of being compromised. Threats to critical energy infrastructure (CEI) are divided into two categories: internal threats and external threats.

According to the European Commission [41], internal threats can be divided into three categories:

- Accidental – like reading a meter incorrectly (which lets the pressure build up too high and could lead to operational problems), not following security protocols as intended or bringing an infected memory stick into the entity.
- Adversarial – like a disgruntled employee who has access to the infrastructure and also knows the structure.
- Structural – like aging equipment, e.g. the East Harlem gas explosion which was attributed to a 127-year-old gas main and led to the termination of gas services to part of the city.

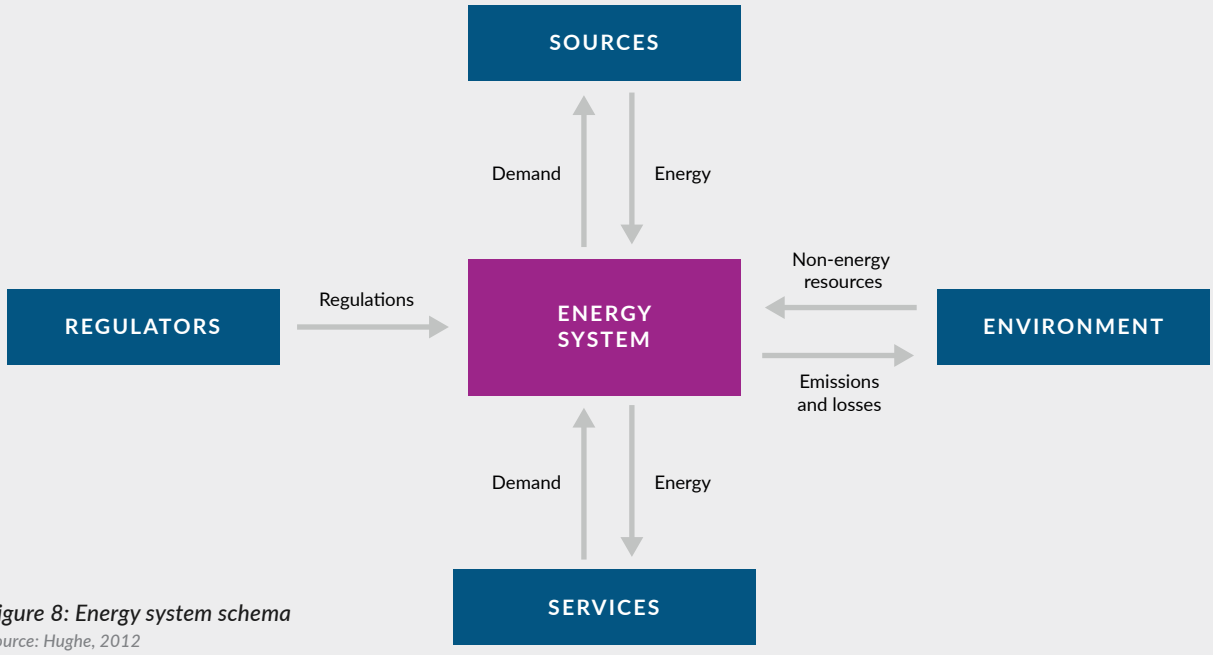

Figure 8: Energy system schema
Source: Hughe, 2012

External threats can be divided into four different sub-categories:

- Accidental – accidents can also cause trouble to CEI, like the 1996 blackout in the US which was caused by a high voltage line touching a tree branch.
- Adversarial – failures owing to adversarial threats are happening more frequently in recent years, especially in the forms of cyberattacks, like the Shamoon malware in 2012 which was used to paralyze and disable the computers of Saudi Aramco oil company. Other forms of adversarial threats include terrorist attacks, sabotage and product tampering.
- Natural disasters – like the 2011 earthquake and the tsunami that followed, leading to the shutdown of Fukushima Daiichi Nuclear Power Plant or big hurricanes like Katrina and Rita, which destroyed offshore rigs and caused a shortage of fuel in the US in 2005.
- Resources – meaning that the source of a particular resource has been completely explored, like the fears surrounding peak oil in around 2008.

Protecting the CEI from the aforementioned threats is vital. Without protective measures from threats the infrastructure could potentially even stop functioning. Authorities need to help an entity to become more resilient. Resilience, according to Moteff [22], is "the ability of a system to resist, absorb, recover from, or successfully adapt to a change in environment or conditions." This resilience can be viewed four different angles: technical, organizational, economic and social [17].

The goal should be to address threats proactively instead of reactively protecting the CEIs. Countermeasures to possible threats will increase the resilience of the systems and decrease the likelihood of these threats actually happening. **Governments and organizations should invest in both physical and cyber risk management products both to reduce risk and to educate employees and plan for organizational resilience** by running the right threat assessments, and be ready to face the threats when they inevitably come.

Transportation is also becoming increasingly "smart", thanks to the help of IoT's capabilities, and equipped with both cyber and physical systems. Advancements like network technologies and sensor networks help in realizing interconnections between different nodes of transport, instantiated as a system of systems [37].

However, technological advancements create challenges related to cybersecurity and high-speed connectivity because of the complexity, heterogeneity and decentralization that characterize these smart transportation systems (STS). There are three main types of challenges when dealing with digital integration of systems in transportation [37]:

1. **The volume and variety of the generated data, l**ike traffic data or sensor data. Successfully managing and utilizing this data can help with efficient monitoring of the physical traffic and achieve real-time responses to any given situation. However, harnessing the full potential of the data is difficult owing to the limited memory space and processing power that any given node of the system has.
2. **Data swapping between the different nodes of the system.** In an STS there is device-to-device contact that allows data transfer. However, swapping data between different IoT systems can be a challenging task, since systems aren't always compatible.
3. **Ensuring the security of the system.** There can be many security challenges in an STS such as low bandwidth and high communication cost. Also, the nodes of the wireless network embedded in the STS may not be physically secured, so may be exposed to unsafe conditions.

According to literature [31], different types of attacks can have a plethora of negative consequences like the ones mentioned in Figure 9. From this table, we can again observe that both cyber and physical attacks seem to plague transportation.

Type of Attack	Description of Attack	Outcome of the Attack
DDoSAttacks	Vehicle to Vehicle message; Electronic Jammin	Chaos on Roadways; Service not available to legitimate users
Revenge and Terrorism	Hacking ITS to get the attacker access to the systems	Driving functions are cooperated and used weapons
System gaming and theft	Hacking the autonomous vehicle	Avoid paying fees and tolls. Stealing goods from vehicle
Physical Attacks	Brute force; Reconnaissance and Man in the Middle attacks	Compromised or Tampered ITS device
Wireless Network Attacks	Sniffs wireless; Jamming of Vehicle security systems; A man in the central of an attack...	Gain access of CAN and on-board diagnostics, infotainment and telematics.
Wired Network Attacks	DNS Spoofing and hijacking; Malware; Spyware; SQL Injection and CSS attacks	Targeted states-sponsored attacks that pose a continuous threat.
VANET Attack	Sybil attacks; Blackhole attacks; Wormhole attacks	Fake location data is transmitted by vehicles; Compromises security-related applications and system.

Figure 9: Type of attacks on transportation
Source: Subhash, 2018

This highlights the importance of both cyber and physical security systems. Different measures that will improve cybersecurity have been proposed [32]. The first is that we need data and models that will help us mitigate the risk. Having the right data will enable the creation of risk models that can help infrastructure managers understand and react better to attacks. Unfortunately, this data isn't readily available. Secondly, metrics for cyber risks need to be developed for the evaluation of different risk management strategies and mitigation measures to be possible. Lastly, scientific literature suggests that cognitive biases routinely result in the underestimation of risk exposure. Those biases can negatively affect decision-making, and we need to understand them and find ways to overcome them. **Systems that allow AI and human cooperation could be a way to mitigate biases.**

NATIONAL SAFETY AND SECURITY POLICE, MILITARY, FIRE, AMBULANCE

As shown earlier, military and other key safety and security organizations like the police or hospitals are among the most common targets of malicious attacks. Threats to national security include those against public military systems but also those against private companies that support government activities and support or operate critical infrastructure [9].

Attacks to a nation's safety and security infrastructures can lead to the loss of sensitive information, damage to the economy and compromised national security. Some examples reported from the US Government Accountability Office that showcase these threats include [9]:

- In 2008, sensitive information from the Department of Defense in the US was compromised, with the use of an infected flash drive which was inserted in a US military laptop at a military base in the Middle East.
- In mid-2009, a research chemist with DuPont, downloaded proprietary information to a personal email account and thumb drive with the intention of transferring this information to Peking University in China.
- In March 2011, an employee of an American company was found guilty of distributing source code that was stolen from the company he was working for. Further investigation revealed that a Chinese company had given that individual $1.5 million to create a control system source code similar to the American company's design.
- In February 2012, a NASA inspector testified that computers with internet addresses from China had gained access to key systems in a NASA laboratory. This allowed them to manipulate sensitive files and infect the system with hacking tools, with the purpose of stealing login credentials and gaining access to more NASA systems.
- In March 2012, hackers gained access to a server with thousands of Medicaid records at the Utah Department of Health. The information accessed included the names of the recipients and the details of children's health insurance plans. Furthermore, around 280,000 people had their Social Security numbers exposed. This led to more than 123,000 people having their personal information accessed. That information included names, addresses, Social Security numbers and other information related to the Government's Thrift Savings Plan (TSP).

Overall, cyberattacks are becoming increasingly dangerous for nations. The FBI ranks the fight against cybercrime as one of its most important law-enforcement activities and nations all over the globe are increasing the budget allocated to cybersecurity.

SMART CITIES

A smart city goes beyond the use of digital technologies for better resource use and less emissions. It means smarter urban transport networks, upgraded water supply and waste disposal facilities and more efficient ways to light and heat buildings. It also means a more interactive and responsive city administration, safer public spaces and meeting the needs of an aging population.

European Commission

Smart cities are another fast-developing area with security issues. According to the European Commission, a smart city is one where traditional networks and services are becoming more efficient by the use of modern digital solutions.

Overall, a smart city integrates smart technology to increase the efficiency, safety and convenience of its services. Some cities that are making use of smart technologies for this purpose include Toronto, New York, Singapore, Paris, Barcelona and Copenhagen [8]. In New York, the city placed hundreds of smart sensors throughout many districts to collect data that will help in trash pickup management. Kiosks that provide people with internet access and charging ports are replacing public phone booths and the New York Police Department (NYPD) is testing web-based software that uses terrain modeling and historical data to predict and respond to crime. Another example is Copenhagen, which received an award in 2017 for a system that monitors traffic, waste management, energy use, air quality and other parameters. The system also connects parking systems, charging systems for selecting vehicles, traffic lights, etc. The data gathered from this system is meant to help in increasing the efficiency of public services [43].

Cities like these, which are actively looking to establish themselves as smart cities, need to address security and privacy issues that can potentially arise from the digital transformation and integration process. Addressing the issues can make the citizens of a city feel more confident and secure, and therefore more willing to participate in the smart city. If citizens are not willing to use the smart features of the city, the whole project can be rendered obsolete, making security a point of paramount significance for the success of a smart city project.

Privacy is a main issue for smart cities, especially as technology is becoming more and more interconnected. For example, a US Supreme Court ruling set a legal precedent on how the US Government's GPS surveillance tracking could violate reasonable privacy expectations. This means that when considering implementations of GPS technologies in smart cities, people also need to think about how to ensure the security and privacy of the citizens' data, and have security up to the required standards [12]. The EU's GDPR legislation can create a similar challenge when planning and implementing digital technologies in Europe.

In their article, Braun et al. [8], present five main security challenges for smart cities:

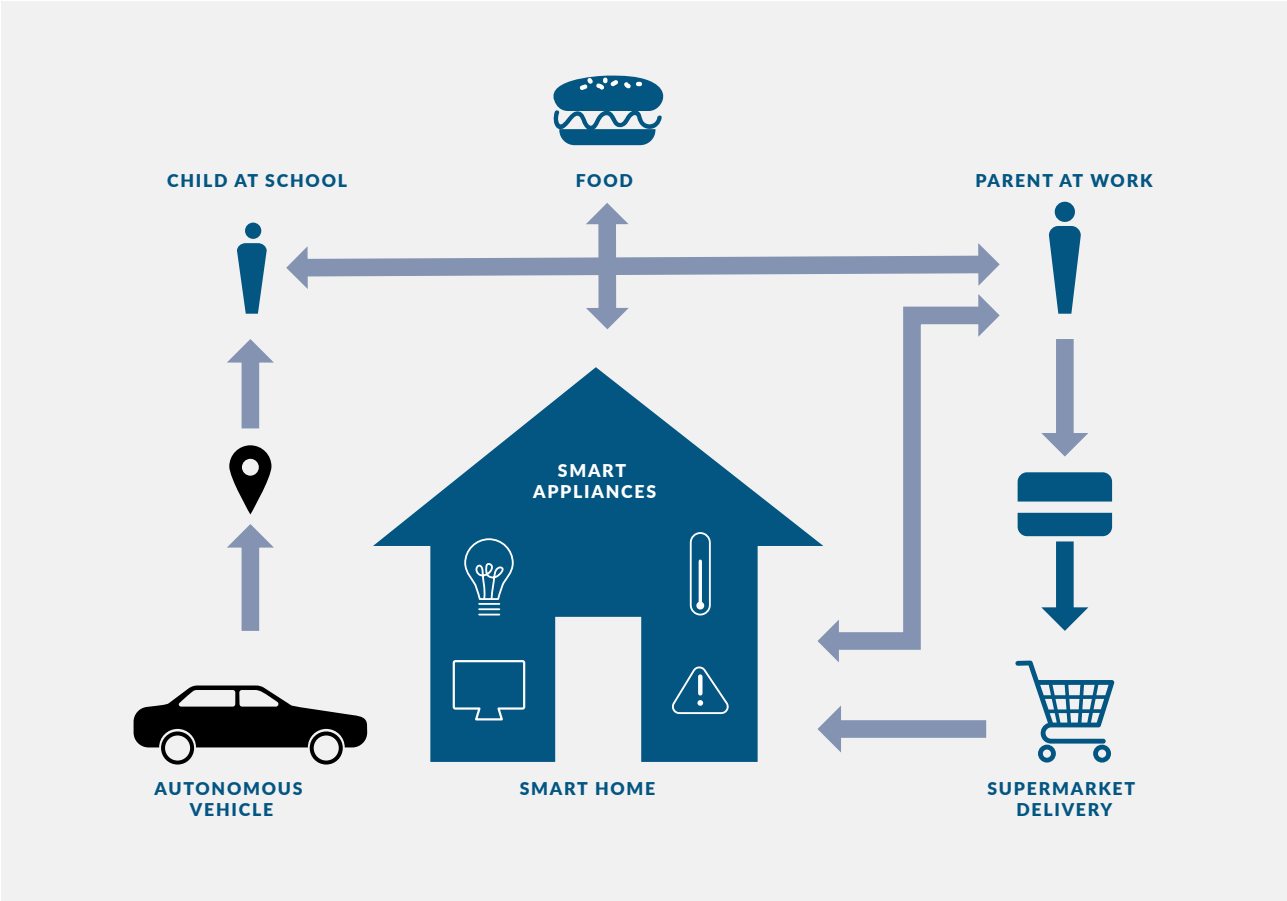

Figure 10: An example of smart city interconnectivity
Source: Braun et al., 2018, p.3

1. **Privacy threats in data sharing and data mining.** How do we ensure personal privacy throughout a smart city that relies on rapid data sharing and data mining techniques with multiple stakeholders?
2. **Privacy threats in data mashup.** Data integration and data mashup in a smart city increase the digital surface in a way that provides more opportunities for security breaches. How will this challenge be overcome?
3. **Cloud security.** What happens to data collected in a smart city? With what specific cloud storage methods is the data collected? How is it secured from cyberattacks? Who is responsible for data breaches? When is it disposed of? Are people going to be able to permanently remove personal data once they are collected?
4. **Secondary use of collected data.** What can the collected data be used for? Can personal data from the smart city and the conclusions drawn from data mining techniques be used commercially? Can consenting individuals provide data that then affects non-consenting individuals?
5. **Threats of artificial intelligence.** How will data mining, machine learning and artificial intelligence (AI) systems in a smart city affect the city's physical safety? To what extent can the data and the data mining techniques dictate the security of a city?

After extended elaboration they conclude that **solutions to the challenges that smart cities face, and are going to face, will be most effective when a holistic approach to security (physical and cyber) and privacy is implemented.**

After reviewing the literature regarding the current state of CNI security and the main challenges the industry faces, we now proceed to a more quantitative analysis of the effectiveness of CNI security and the benefits it can offer, not only to the CNI industry but also to the economy in general.

Owing to data availability, we chose to focus specifically on the impact of cybersecurity on the CNI industry and the economy overall. The issue was examined from three different angles:

1. How cybersecurity impacts critical infrastructure, specifically the transport, storage and communication industry (Model #1).
2. How cybersecurity impacts investments in critical infrastructure, specifically the investments in energy (Model #2).
3. The overall impact that both cybersecurity and digital development can have on economic growth (Model #3).

The specific industries were again chosen because of data availability and are essentially used as a proxy for the whole CNI industry. If the results of the models showcase positive relations between cybersecurity and the aforementioned industries, this provides a strong implication that the relations will also be positive for the CNI industry as a whole, since CNI security shares many similarities across different industries.

This part of the paper presents the hypotheses, methodology and results of the modeling.

Basic hypotheses and conceptual models

Basic hypotheses for Model #1

First, we examined how cybersecurity can directly impact critical infrastructure. For this purpose, the transport, storage and communications industry was chosen because of relevancy and data availability. As discussed earlier, ensuring the security of the modern transportation network is a major challenge because of the many different smart systems at work. In the available scientific literature, there are different papers that support the idea that cybersecurity is positively connected with sustainable economic growth, and is a major differentiator for organizations [16,34].

Based on these academic findings, this white paper formulates the following first hypothesis:

1a. A country's cybersecurity is positively correlated with the added value that its transport, storage and communications industry provides.

Of course, cybersecurity is not the only factor that affects the industry. Other factors like the infrastructure of each country will affect the industry's output. According to the literature, there is a positive link between infrastructure – specifically transportation and communication infrastructure – and economic growth [15,11,18,26]. So, in order to create a more complete model and include the impact of infrastructure in the analysis, the following second hypothesis was formulated:

1b. A country's infrastructure is positively correlated with the added value that its transport, storage and communications industry provides.

Based on the two aforementioned hypotheses, the following conceptual model was defined.

Model #1: $log(avbt_i) = b_2 log(csi_i) + b_2\, log(ti_i) + e_i$

where:

- avbt = added value to the economy of a country by the transport, storage and communications industry in US dollars
- csi = a county's cybersecurity index based on the National Cyber Security Index (NCSI)
- ti = a country's transportation infrastructure based on World Bank's Logistics Performance Index (LPI).

Basic hypotheses for Model #2

In the second model we are interested to see if cybersecurity can have a positive impact on CNI investments. As a proxy to examine this, we are going to use the energy industry and see whether or not cybersecurity is correlated with investments.

There is evidence in the literature that stability is a key factor that contributes to energy investments [20]. Generally speaking, stability in a country positively impacts investments. Also, risk related to technology has been shown to negatively impact investments [21]. Based on this, we feel confident formulating the following hypothesis:

2. A country's/organization's cybersecurity level is positively correlated with investments in energy.

Based on this hypothesis, the following conceptual model was defined.

Model #2: $log(EI_i) = b_2 log(csi_i) + e_i$

where:

- EI = a country's energy investments (private and public participation) in US dollars
- csi = a county's cybersecurity index based on the NCSI.

Basic hypotheses for Model #3

After examining the effect of cybersecurity on part of the CNI industry, a more general question occurred. Cybersecurity is only one aspect that can affect the economic output of an industry. It would also be interesting to investigate the relationship between digital growth and economic growth. A similar methodology with the previous model was used.

Many papers have examined the relationship between technology and economic growth. Although someone might expect that this relationship would always be positive, that is not the case. One negative aspect of the implementation of new technologies is that it can increase inequality inside the economy. Technological developments affected the structure of wages and determined an increase in income inequality in most developed nations [1]. There can also be a negative link between internet adoption and growth for countries with high income inequality [24]. The most interesting finding, though, is that a study found that science and technology graduates negatively influence real GDP growth in EU-28 and that the effect of the internet in terms of subscribers and users negatively influences real GDP growth in EU-28 [4]. Based on those findings, the following hypothesis was formed:

3a. A country's/organization's digital development level is negatively correlated with its GDP growth rate.

Also, thinking along the same lines as in Model #1, and using the same bibliographical references [16,34], we can make the second hypothesis:

3b. A country's/organization's cybersecurity index is positively correlated with its GDP growth rate.

Based on the two aforementioned hypotheses, the model that was created is as follows:

Model #3: $AGR_i = b_i ddl_i + b_2\, csi_1 + e_2$

where:

- AGR = average growth rate based on World Bank data
- csi = a county's cybersecurity index based on the NCSI
- ddl = a country's digital development level based on NCSI ratings.

Data description

To test the above hypotheses, existing data from reputable sources were used.

In order to define the size of the transport, storage and communications industry per country, we used data from the United Nations Statistical Office. These data are represented in US dollars.

For measuring cybersecurity, we used the NCSI, which is publicly available on https://ncsi.ega.ee. The purpose of the index is to measure the "preparedness of countries to prevent cyberthreats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cyber security capacity building." The index is built based on the national cybersecurity framework, as can be seen in Figure 11. It gives a score from 0 to 100 for every country. For more information on

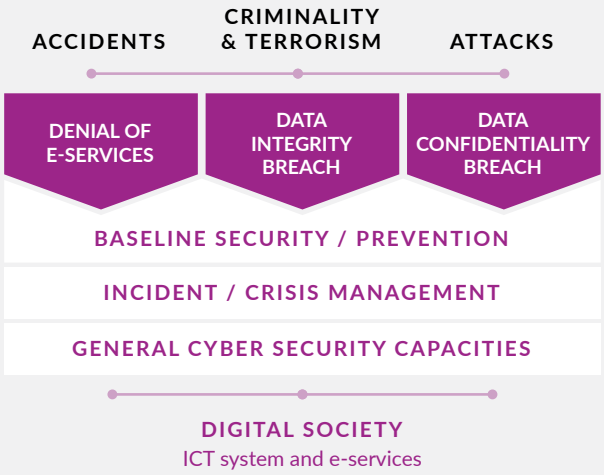

Figure 11: NCSI framework (place holderJF)
Source: NCSI website

how the index is calculated and what it takes into consideration, you can refer to the NCSI website. The index is used as a proxy for each country's cybersecurity capabilities.

For each country's level of transportation infrastructure, data from the World Bank were used. More specifically, the transportation infrastructure score that is part of the World Bank's LPI (Logistics Performance Index) was used.

For each country's energy investments, again data from the World Bank were used. The data were expressed in current US dollars in 2020.

The data for the average growth rate from 2014–20 for each country was calculated using data from the World Bank.*

After omitting countries that weren't present in all of the above indexes, there were 125 countries in the data set for Model #1, 58 countries for Model #2 and 147 countries for Model #3.

Methodology

An Ordinary Least Squares regression (OLS) was created to estimate the coefficients between the independent variables (IV) of the models (cybersecurity and transportation infrastructure, etc.) and the dependent variables (DV) (added value in the economy from transport, storage and communications, energy investments and GDP growth). This method uses the minimum squared error (SSE) for the estimates and its general form for a model with, let's say, p explanatory variables as follows:

$$Y = \beta_0 + \sum_{-j=1..p} \beta_j X_j + \varepsilon$$

where Y is the dependent variable, β_0, is the intercept of the model, Xj corresponds to the jth explanatory variable of the model (j= 1 to p), and ε is the random error with expectation 0 and variance σ^2.

It is generally accepted that OLS regression has multiple advantages including its simple implementation, the fact that it performs well on linearly separate data sets and the fact that it can reduce overfitting – a problem most commonly occurring when ml modeling methods are used.

A Wald Chi-square test was used to evaluate the quality of the models. The test returned values less than the critical for all three models, meaning that the assumptions that the models predict better than the null model hold, and the models are adequate.

**World bank growth rate data: Annual percentage growth rate of GDP at market prices based on constant local currency. GDP is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources.*

Table 1: Chi-Squared Test

Model #1	X2= 819.4	df = 2	P(>X2) =0.0
Model #2	X2 = 148.9	df = 1	P(> X2) = 0.0
Model #3	X2= 45.7	df = 2	P(> X2) = 0.00000000012

For models #1 and #3 that have more than 1 independent variable, multicollinearity for the variables used was also addressed. A VIF (Variance Inflation Factor) scores test was used to ensure that multicollinearity was not a problem. This allows for correct interpretation of the results. The VIF scores in both cases were less than 3, meaning that there is not a multicollinearity issue.

Table 2: VIF Scores

	log(csi)	log(ti)	ddl	csi
Model #1	1.874029	1.874029	-	-
Model #3	-	-	2.198828	2.198828

Regression results

In this part the outputs of the models are going to be presented.

Model #1 results

As we can see, both independent variables have a positive impact on the transport, storage and communications industry. The model is analytically presented in the Table 3. Because the model is a log-log model, meaning that both IVs and DV are in logarithmic form, the results can generally be interpreted as $\%\Delta y = \beta 1 \%\Delta x$. This means that if the cybersecurity index of a country is increased by 1% then the added value to the economy from the transport, storage and communications industry will increase almost by 0.57%. We see the same thing with the transportation infrastructure. If the ti index of a country is increased by 1% then the added value from the industry will increase by almost 5.16%.

Table 3: Model #1 – regression outputs

Coefficients:	Estimate	Std. Error	t value	Pr(>|t|)	
(Intercept)	15.3806	0.6640	23.165	<0.0000000000000002	***
log(csi)	0.5697	0.2329	2.446	0.0159	*
log(ti)	5.1571	0.7502	6.875	<0.000000000283	***

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
Adjusted R2 = 0.5318

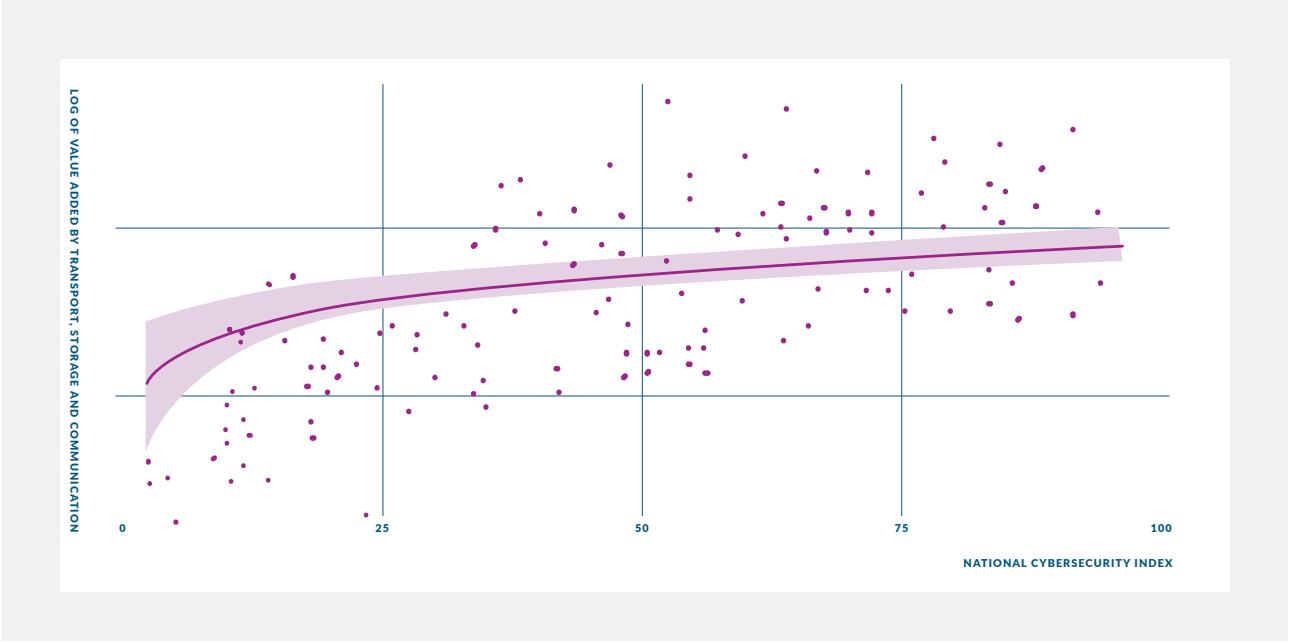

Figure 12: Model #1 scatter plot

To put the results into perspective, a 0.57% increase doesn't sound like much – but considering the size of the transport, storage and communications industry we can see that it is not negligible. In North America, for example, a 1% increase in the NCSI, meaning an increase in cybersecurity, can lead to an increase in added value up to $12.34 billion. In the diagram below we can see a scatter plot that showcases the positive slope of the relationship between cybersecurity and the industry.

Essentially what we see is that **the ability to increase cybersecurity levels can have multiple economic benefits.**

Model #2 results

Looking at the second model we can see that the relationship between cybersecurity and energy investments is positive and statistically significant. This model is again a log-log model, so the interpretation of the results goes as follows: if there is going to be an increase of 1% on the cybersecurity level, a corresponding increase of 0.85% is going to be observed on energy investments. This means that an increase in cybersecurity levels can positively affect the economy.

Table 4: Model #2 – regression outputs

Coefficients:	Estimate	Std. Error	t value	Pr(>|t|)
(Intercept)	3.56484	1.3384	12.202	0.0000000000000226***
log(csi)	0.8509	0.3787	2.247	0.0319*

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Adjusted R2 = 0.056

According to the International Energy Agency (IEA), investments in energy are expected to reach $1.9 trillion in 2021. This means that an increase of 1% on the cybersecurity index can add up to $16.17 billion on energy investments.

There are two possible explanations for this. The first is that an increase on the cybersecurity index is reducing risk and makes investors feel more confident. This is in line with the literature that we reviewed. Another reason could be that a part of investments is directed toward cybersecurity, creating a kind of secular relationship between those variables.

Model #3 results

As can be seen in Table 5, both of the variables are statistically significant. The digital development level is negatively affecting the economy, confirming the first hypothesis. On the other hand, the cybersecurity level is positively correlated with economic growth. Here we see again that an increase in cybersecurity levels can positively affect the economy.

Table 5: Model 3 – regression outputs

Coefficients:	Estimate	Std. Error	t value	Pr(>|t|)	
(Intercept)	3.56484	0.55748	6.395	0.00000000211	***
ddl	-0.04846	0.01494	-3.243	0.00147	**
csi	0.02297	0.01075	2.137	0.03427	*

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Adjusted R2 = 0.056

While interpreting the above results, try to think of it as a cybersecurity surplus or deficit. The more digitally advanced a nation/organization is, the better cybersecurity it needs to have in order to benefit from the new digital technologies it is implementing. If not, the new digital technologies can actually have a negative impact on economic growth. **This can happen because of many different factors, including the fact that cyberattacks on new digital systems can lead to interruptions and stall growth. For a country or organization to be able to harness the power of new digital technologies, a corresponding level of security needs to be in place.**

CONCLUSIONS AND RECOMMENDATIONS

The global CNI industry is constantly facing multiple security challenges. As malicious attacks become more common, but at the same time more complex, no specific industry can claim to be free from the threat of attack. **The integration of the different security systems that a facility is using is a key factor for success. The implementation of AI technology has the potential to greatly improve cyber-physical security capabilities and also increase industry profitability.**

Our economic modeling suggests that in the transport, storage and communications industry, this can be as big as $36 billion globally for each incremental improvement in cybersecurity. We also found that better cybersecurity can lead to higher investments in the energy industry. These results suggest that **the economic benefits of improving cybersecurity are multifaceted and extended to the CNI industry as a whole.**

This opportunity presents itself at a critical time as the global economy is aiming to recover from the Covid-19 crisis, while it is also dealing with the war in Ukraine and the inflation caused by the global supply chain crisis. To achieve an economic boost, increase organizational resilience and get ahead of the competition, **CNI companies need to invest in integrated cybersecurity solutions that make use of new technologies and AI.**

As already mentioned, the goal of countries and organizations should be to proactively address cyber-physical threats instead of reactively protecting their facilities. Countermeasures to possible threats will increase the effectiveness of the security systems and will decrease the likelihood of these threats actually happening. **Governments/organizations should invest in both physical and cyber risk management products in order to reduce risk. But they must also educate employees and plan for organizational resilience by running the right threat assessments, and be ready to face the threats when they inevitably come.** Integrated security solutions that also have AI capabilities can mitigate human biases and increase security effectiveness. A holistic, integrated approach to security can increase the effectiveness of existing security solutions too.

Threats to CNI are growing exponentially and are becoming increasingly dangerous for nations. The damages and costs of a successful attack can also be very high, according to the various third-party reports that were discussed – as high as multiple million dollars per attack. As our modeling showcases, **the more digitally advanced a nation/organization is, the better cybersecurity it needs to have in order to benefit from the new digital technologies it is implementing.**

In times like these, when the global economy operates under many uncertainties, it is next to impossible to predict the future. But by building organizational resilience, you can be prepared for unexpected obstacles**. Investing in cyber-physical security can mitigate risks, reduce losses and damages and potentially lead to faster growth.**

Cyber-physical security (CPS) in CNI is an issue of paramount importance. The CPS systems in place guard against major economic disruption and even threats to human life. This paper has analyzed the current state and found cyber-physical threats growing in scope and complexity.

Nations and organizations need to raise their game in response to this threat. Holistic systems--level thinking is needed, rather than the silo approach often found in technology architecture. Management of the entire digital and physical system from end to end is required, using advanced technology such as AI.

The original modeling in this paper proves that the right investments in cyber-physical systems will unlock tremendous economic value. Billions of dollars of value across key regions such as North America, India and the Middle East can be realized through effective leading-edge CPS systems. Conversely, failure to invest and upskill in cyber-physical systems opens major risks with potential large-scale economic consequences.

THE SPONSOR OF THIS REPORT

Commtel Networks is a global engineering and technology company providing unified critical communication, along with surveillance, security, safety, and AI solutions for clients in the oil and gas, power, mining, transportation and other Critical National Infrastructure sectors. Commtel is at the forefront of engineering intelligence, with expertise in executing turnkey solutions – design, engineering, multi-system integration, project management, commissioning and life cycle management. Founded in 1998, Commtel has delivered over 500 projects across four continents, enabling the digital transformation of its clients' mission-critical infrastructure.

CN-SHIELD, a new approach for critical asset protection from Commtel

CN-SHIELD is an AI software solution that unifies all assets, monitors and assesses the data, and implements faster and cohesive 360-degree protection. It enables novel ways to deal with the threats associated with the present-day cyber-physical systems. It provides customers with the power to collect data from myriad devices and systems on a single data processing platform, allowing you to predict a situation, prevent a mishap, and helps the preservation of all mission-critical systems.

SECURITY of a facility, SAFETY of human assets, SURETY of availability of all assets – the ability of the platform to perform this function across disparate systems to enhance the protection of a CNI will be first of its kind and will drive substantial economic value.

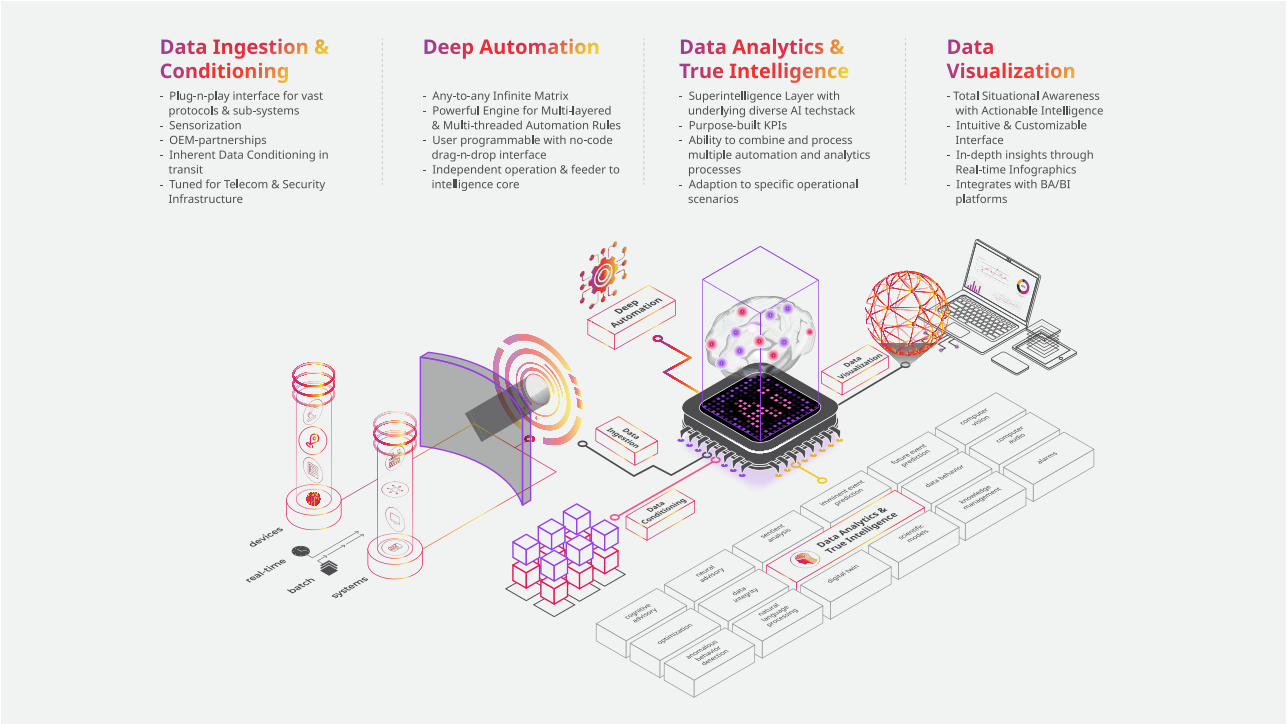

Figure 13: CN-Shield framework

CN-SHIELD as an augmented supervision and intelligent management solution

According to everything researched so far, both qualitative and quantitative, there are three main issues in modern CNIs that the implementation of this system can help with:

1. **Integration of many separate security systems, both cyber and physical.** On this point the literature is very direct. Many different security systems are hard to manage all at once; integration can help with efficiency and ease of use. Also, human biases have been proven to negatively affect CNI security decisions. As discussed in the paper, most information security higher-ups feel highly confident in their organization's security capabilities, but most of the time their security – specifically the cyber part of it – is eventually compromised. The CN-SHIELD solution can help with mitigating biases and can improve CNI security performance.
2. **Better management of big data generated by systems.** Another issue that kept popping up is the challenges in managing the big data that is constantly produced by modern systems. CN-SHIELD has functions for collecting, storing and reporting on this data.
3. **Improve the overall cyber-physical security that will lead to better performance through its AI-based decision-making and decision-executing system.** The improvements in cyber-physical security can offer many benefits to countries and corporations, both in terms of security risk reduction and in terms of economic benefits, as our modeling showed.

SOURCES

Literature

1. Acemoglu, D. (2002). Technical change, inequality, and the labor market. Journal of Economic Literature, 40(1), 7–72.
2. Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cybersecurity incidents: A review cases in cyber-physical systems. International Journal of Advanced Computer Science and Applications, (1), 499–508.
3. Alexander, K. B. (2007). Warfighting in cyberspace. National Defense, University of Washington DC Institute for National Strategic Studies.
4. Armeanu, D. Ş., Vintilă, G., & Gherghina, Ş. C. (2017). Empirical study towards the drivers of sustainable economic growth in EU-28 countries. Sustainability, 10(1), 4.
5. Ben Naseir, M. A., Dogan, H., Apeh, E., Richardson, C., & Ali, R. (2019, April). Contextualising the national cyber security capacity in an unstable environment: A spring land case study. In World Conference on Information Systems and Technologies (pp. 373–382). Springer, Cham.
6. Berdibayev, R., Gnatyuk, S., Yevchenko, Y., & Kishchenko, V. (2021). A concept of the architecture and creation for SIEM system in critical infrastructure. In Systems, Decision and Control in Energy II (pp. 221–242). Springer, Cham.
7. Bernik, I. (2014). Cybercrime and Cyber Warfare. John Wiley & Sons.
8. Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. Sustainable Cities and Society, 39, 499–507.
9. Clark, R. M., & Hakim, S. (eds; 2016). Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level (Vol. 3). Springer.
10. Critchley, T. (2014). High Availability IT Services. CRC Press.
11. Egert, B., Kozluk, T. & Sutherland, D. (2009). Infrastructure and growth: empirical evidence. CESifo Working Paper No. 2700.
12. Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research, 5(4), 491–497.
13. Etesami, S. R., & Ba□ar, T. (2019). Dynamic games in cyber-physical security: An overview. Dynamic Games and Applications, 9(4), 884–913.
14. EY (2017). Global Information Security Survey, December 2017.
15. Kopp, A. (2007). Macroeconomic productivity effects of road investment: A reassessment

for Western Europe, Transport Infrastructure Investment and Economic Productivity. Report of the 132nd Round Table on Transport Economics.

16. Kshetri, N. (2016). Cybersecurity and development. Markets, Globalization & Development Review, 1(2).
17. Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. Technological Forecasting and Social Change, 103, 21–33.
18. Lavee, D., Beniad, G., & Solomon, C. (2011). The effect of investment in transportation infrastructure on the debt-to-GDP ratio. Transport Reviews, 31(6), 769–789.
19. Mallick P. K. (2021). Cyber weapons – A weapon of war? Vivekananda International Foundation.
20. Maniruzzaman, A. F. M. (2008). The pursuit of stability in international energy investment contracts: A critical appraisal of the emerging trends. Journal of World Energy Law & Business, 1(2), 121–157.
21. Masini, A., & Menichetti, E. (2012). The impact of behavioural factors in the renewable energy investment decision making process: Conceptual framework and empirical findings. Energy Policy, 40, 28–38.
22. Moteff, J. D. (2012). Critical infrastructure resilience: The evolution of policy and programs and issues for congress.
23. Muller, L. P. (2015). Cyber security capacity building in developing countries: Challenges and opportunities.
24. Noh, Y. H., & Yoo, K. (2008). Internet, inequality and growth. Journal of Policy Modeling, 30(6), 1005–1016.
25. Hughes, L. (2012). A generic framework for the description and analysis of energy security in an energy system. Energy Policy 42, 221–231.
26. Park, J. S., Seo, Y. J., & Ha, M. H. (2019). The role of maritime, land, and air transportation in economic growth: Panel evidence from OECD and non-OECD countries. Research in Transportation Economics, 78, 100765.
27. Pawlak, P. (2016). Capacity building in cyberspace as an instrument of foreign policy. Global Policy, 7(1), 83–92
28. Spremić, M. (2015). Corporate governance of enterprise IT: Research study on IT governance maturity. International Journal of Economics and Management Engineering, 9(9), 3071–3075.
29. Spremić, M. (2018): Enterprise information system in digital economy. Faculty of Economics and Business, Zagreb, Croatia.
30. Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 341–346).
31. Subhash, M. B. (2018). A survey on intelligent transportation security systems. International Journal of Computer Science Trends and Technology (IJCST) – 8(4), Jul–Aug.
32. Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. Transport Policy, 79, 103–114.
33. Tyagi, A. K., & Sreenath, N. (2021). Cyber Physical Systems: Analyses, challenges and possible solutions. Internet of Things and Cyber-Physical Systems, 1, 22-33.
34. Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an essential sustainable economic development factor. European Journal of Sustainable Development, 7(4), 171–178.
35. Von Solms, B. (2006). Information security – the fourth wave. Computers & Security, 25(3), 165–168.
36. Yu, W., Zhang, N., Fu, X., & Rivera, B. (2012). Evolution of widely spreading worms and countermeasures: Epidemic theory and application. In Handbook on Securing Cyber-Physical Critical Infrastructure (pp. 73–93). Elsevier Inc.
37. Zhang, J., Wang, Y., Li, S., & Shi, S. (2020). An architecture for IoT-enabled smart transportation security system: A geospatial approach. IEEE Internet of Things Journal, 8(8), 6205–6213.

Web

38. Centre for the Protection of National Infrastructure (2021, April 20). Critical National Infrastructure. https://www.cpni.gov.uk/critical-national-infrastructure-0
39. Clover Jack (2022, Jun 18) Russian spies could be 'active at all levels of British society', MI5 believes. Mirror. https://www.mirror.co.uk/news/uk-news/russian-spies-could-active-levels-27269533
40. Cloudflare. What is a DdoS attack? https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
41. European Commission. Smart cities. https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en
42. Fortinet. Trojan Horse virus. https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus
43. Kosowatz John (2020, Feb 3) The top 10 growing smart cities. The American Society of Mechanical Engineers. https://www.asme.org/topics-resources/content/top-10-growing-smart-cities
44. Muncaster Phil (2021, Nov 10). Over 80% of CNI firms have been breached in past 36 months. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/over-80-cni-firms-breached-past-36/
45. Norton. What is a computer virus? https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
46. Purplesec (2022). Cyber security statistics: The ultimate list of stats, data, & trends for 2022. https://purplesec.us/resources/cybersecurity-statistics/#:~:text=From%202016%20through%202020%2C%20between,2021%20were%20zero%2Dday%20attacks
47. RISI Online Incidents Database (2015, Jan 28). https://www.risidata.com/Database
48. UK Parliament (2021, Apr 29). Physical threats to infrastructure. https://post.parliament.uk/physical-threats-to-infrastructure/
49. Weinberg Adam (2021, Jun 2). Analysis of top 11 cyber attacks on critical infrastructure. https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
50. Yahoo Finance (2021, Nov 12). 83% of critical infrastructure organizations suffered breaches, 2021 cybersecurity research reveals. https://finance.yahoo.com/news/83-critical-infrastructure-organizations-suffered-000500692.html

Other reports:

51. IBM (2021). Cost of a data breach report. https://www.ibm.com/security/data-breach
52. Ponemon Institute (2019). The cost of cybercrime. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf