University of Kent

Kent Academic Repository

Yuan, Haiyue and Li, Shujun (2022) *Cyber Security Risks of Net Zero Technologies.* Technical report. University of Kent, Kent, UK

Downloaded from

https://kar.kent.ac.uk/115370/ The University of Kent's Academic Repository KAR

The version of record is available from

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

OGL (Open Government Licence)

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in ***Title of Journal*** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

Cyber Security Risks of Net Zero Technologies

Haiyue Yuan and Shujun Li

Institute of Cyber Security for Society (iCSS) & School of Computing
University of Kent, Canterbury, Kent, UK
Email: {h.yuan-221, s.j.li}@kent.ac.uk

April 11, 2022



Abstract

This report is the outcome of a piece of contracted research done for the DCMS (Department for Digital, Culture, Media and Sport) of the UK Government in 2022, in the hope to provide useful insights for future policy reviews and changes related to cyber security risks of the so-called "net zero technologies", technologies that can help the UK and the world achieve the "net zero" greenhouse gas (GHG) emission goal by 2050. The report first reviews the general background about the NZ goal and sectors involved in NZ technologies, and then focuses on a broad analysis of cyber security risks and solutions related to NZ technologies, from both technological and socio-technical aspects. The report concludes with a list of identified open challenges that require more future research and development, and some recommendations to the DCMS and all relevant stakeholders playing a role on NZ technologies. The report also includes an appendix explaining our research methodology briefly, another one listing some selected researcher groups, centres and projects working on NZ technologies, and a third one listing some relevant scientific journals and magazines.

1 Introduction

1.1 General Background

The Intergovernmental Panel on Climate Change (IPCC) assessed around 6,000 peer-reviewed publications and produced the 2018 "Special Report on Global Warming of 1.5°C" [29]. This report states that climate change has been affecting the ecosystem and livelihoods all around the world. Therefore, it is necessary to limit the global warming to 1.5°C above pre-industrial levels to significantly reduce the foreseeable public health

© 2022 Crown copyright

catastrophes. The general recommendation to achieve this is to lower the human-caused carbon dioxide (CO_2) emissions to approximately a half of 2010 levels by 2030 and to net-zero (NZ) by 2050. In addition, the emissions of all greenhouse gases (GHGs) must achieve NZ thereafter between 2063 and 2068. The International Energy Agency (IEA) defines NZ emissions as "a balance between anthropogenic emissions by sources and removals by sinks of greenhouse gases" [9], meaning that it is not simply the complete decarbonisation but rather compensating anthropogenic GHGs to achieve an equilibrium between absorption and emission.

To win this global goal for NZ emissions, governments around the world have made commitment to take actions collaboratively. As the first country to pass an NZ emission law, the UK Government has set its commitment to achieve its NZ GHG emission goal by 2050 [48], and Scotland committed to achieve the goal five years earlier – by 2045 [41]. As a recent landmark event, the UK hosted the United Nations Framework Convention on Climate Change (UNFCCC) Conference of the Parties (COP 26) in Glasgow from 31 October to 12 November 2021, which brought together almost 200 countries to attend and to agree on the Glasgow Climate Pact (GCP) that aims at accelerating global actions on achieving the NZ goal [50]. The GCP emphasises that it is crucial for all sectors and all parts of the global society to collaboratively deliver effective climate actions [51].

In order to achieve the NZ emission goal, technologies that can help reduce emissions of CO_2 and other GHGs, which are often called "NZ technologies". To the best of our knowledge, there is no established consensus among nations and different stakeholders on the precise definition of NZ technologies. Many reports and research articles use a phrase like 'technologies helping achieve the NZ emission goal' to describe the concept. For the purpose of this report, we decide to use a broader concept "NZ-related technologies" to indicate different relationships between relevant technologies and the NZ goal: 1) *NZ-enabling technologies* that can help reduce GHG emissions, which can be understood the narrow-sense NZ technologies; 2) *NZ-unfriendly technologies* that can increase GHG emissions *directly*, whose use should be limited or eventually discarded (at least when being used alone); 3) *NZ-neutral technologies* that are not directly related to controlling GHG emissions but may negatively or positively affect GHG emissions or the performance of other NZ-related technologies directly or indirectly. Note that the term "technologies" itself is also quite vague, as the boundary between technologies, systems and ecosystems is not a clear cut. When multiple NZ-related technologies are used in a large system, an NZ-neutral or -unfriendly technology may help achieve a positive sum – reducing the overall GHG emissions of the whole system, therefore turning itself to an NZ-enabling technology. We will use blockchain technologies as an example to illustrate this point later in this report.

1.2 Important NZ Sectors and NZ-Related Technologies

Many stakeholders in different sectors can contribute and need engaging to achieve the NZ goal. Here, we discuss some important sectors that are often highlighted in discussions on the NZ goal and NZ-related technologies.

© 2022 Crown copyright

1.2.1 Energy

One of the most discussed and highlighted NZ-related sectors is *energy*. This sector is particularly important because less renewable forms of energy are one of the major sources of GHG emissions, e.g., less sustainable fuels used in the transport sector. How to increase the use of more renewable energy sources and how to reduce the GHG emissions of less renewable ones have been considered as two of the key components in NZ strategies of different nations and sectors. Important NZ technologies for more renewable energy generation include bioenergy technologies, geothermal technologies, hydropower technologies, ocean technologies, solar technologies, and wind power technologies [1]. Within the larger energy sector, several important sub-sectors are often considered in NZ actions: *energy generation*, *energy storage and transmission* (e.g., *battery*), *fuel* (particularly, *oil and gas*), and *electricity* (including *electricity generation* and *electricity grid* for electricity transmission and load control).

It is important to note that the shift to more renewable energy requires incentivising not only the energy sector but also *energy consumers* (e.g., using financial, legal and regulatory levers to encourage consumers to adopt more renewable forms of energy). Since energy consumers cover all sectors and citizens, including the energy sector itself (which needs to consume energy as well), energy-related NZ efforts are often *cross-sectoral* by nature and therefore require cross-sectoral collaboration and coordination. From energy consumers' perspectives, an important direction of NZ efforts is about *energy saving technologies*. Notable examples include *green ICT (information and communication technologies)*, *AI-based energy saving technologies*, and *more energy-efficient building (including manufacturing plants, office and residential buildings) and vehicles*.

NZ efforts on more renewable energy sources focus more on reducing GHG emissions in the energy generation and consumption processes. Another important area is about reducing GHG emissions in the transmission processes and reducing GHG emissions into the atmosphere after they are produced. NZ technologies in these areas can be independent of the form of energy, e.g., an important new industrial sector on *carbon capture, utilisation and storage (CCUS)* has emerged, where new NZ technologies are being developed to reduce emitted CO_2 into the atmosphere [35, 56]. NZ technologies for energy transmission rely more on the specific form of energy transmitted, e.g., the use of smart grid to optimise the whole life cycle of electricity generation, transmission, consumption, transformation, load control, storage, re-distribution, etc. [16]. The shift to low-carbon energy systems also sees the development of new NZ technologies to facilitate the transition of the traditional energy distribution/network/grid to smart grid, micro-grid, multi-vector energy network, etc. [10, 16, 28, 37, 45].

1.2.2 Transport & Tourism

One of the most important sectors relevant for NZ technologies is *transport*. According to a 2016 report of the European Environment Agency (EEA) [12], the largest carbon emitter in Europe from 2006 to 2016 was the transport sector, where more than 70% of the emissions came from passenger cars. This is the case for the UK as well: according to the Department for Transport's 2021 annual report on transport and environment statistics [34], transport was the largest emitting sector of GHGs in the UK, with 27%

© 2022 Crown copyright

of the whole country's total emissions in 2019. Note that the transport sector is also a major consumer of different forms of energy, so has a lot of connections with the energy sector (as mentioned above in the previous sub-subsection). Important NZ technologies for transport include electric vehicles (EVs), hydrogen-powered vehicles, intelligent transport systems (ITSs), and mobility-as-a-service systems, which have all attracted a lot of attention from relevant stakeholders including different industry sectors (not limited to transport), governments (both national and local, and cross-governmental bodies), consumers, and researchers from many disciplines.

Note that the transport sector overlaps another sector – *tourism*. A 2018 research paper [24] estimated that tourism is responsible for around 8% of the global carbon emission, with nearly half due to tourism-related travel/transport. In addition to using general NZ-enabling technologies, e.g., more sustainable forms of energy, more energy-saving technologies, and carbon offset trading systems, we (the authors of this report) believe that *virtual tourism* (e.g., leveraging virtual reality technologies) can be a new emerging direction that can help reduce carbon emission, potentially substantially.

1.2.3 Agriculture & Food

Another NZ-related sector that often surprise many people is agriculture. A 2020 report commissioned by the BEIS (Department for Business, Energy & Industrial Strategy) [39] estimates the overall GHG emission contribution of the agriculture sector in the UK was 10%. At a global level, the contribution seems higher, e.g., according to a 2013 report from the Food and Agriculture Organization of the United Nations [32], global GHG emissions caused by animal farming was roughly equivalent to the global transport sector. Similarly, a 2020 report from Greenpeace [33] found out that GHG emissions caused by animal farming has been increasing, and that, when both direct and indirect emissions are counted, animal farming in the EU produced more emissions than those produced by cars and vans combined. Those figures suggest that both at the national (UK) and global levels, agriculture is indeed an important sector for the NZ goal.

Addressing GHG emissions of this sector is more complicated because it supports food supplies to the global population and other complicated matters such as connections between modern agriculture and deforestation [31]. Note that the agriculture is part of the much larger food industry, which extends to many other sectors such as manufacturing, food processing and food distribution.

1.2.4 ICT

A very special sector playing a unique role in the NZ context is *ICT (information and communication technologies)* (also called digital technologies, although this term has a flavour to be narrower than ICT). Modern ICT technologies are increasingly transforming many sectors and the whole human society into a highly digitalised world, in which people, organisations, hardware devices, software systems, data, processes and also different types of (smart) things are all connected in an Internet of Everything (IoE) [23].

While becoming an essential part of many sectors, ICT technologies have also been widely used to help reduce GHG emissions in different ways. Some indicative examples of NZ-enabling technologies include: 1) using smart sensing technologies based on AI

© 2022 Crown copyright

and wireless sensor networks (WSNs) to help optimise the use of energy by end users to directly save energy and therefore reduce emissions in many sectors; 2) using AI, 5G telecommunication Internet of Things (IoT) and distributed database (e.g., blockchain) technologies to help support better transport planning, routing and travel-related decision making to directly reduce emissions associated via improved the energy efficiency of (fuel-based and electric) vehicles; 3) leveraging modern industrial control systems (ICSs) and Supervisory Control and Data Acquisition (SCADA) systems to improve energy efficiency of manufacturing processes in different industrial sectors; 4) providing more advanced information management processes to facilitate NZ-related decision making processes to directly or indirectly help reduce emissions.

In addition to ICT technologies serving as an enabler, the development of more environment-friendly ICT technologies has also attracted a lot of interests from different stakeholders, under terms such as *green ICT* or *green computing*. Green ICT technologies can be broadly split into two categories: more energy-efficiency ICT technologies (e.g., AI algorithms with a lower computational complexity), and ICT technologies for energy saving purposes (e.g., smart sensing technologies that help reduce energy consumption of ICT systems themselves).

The ICT sector is unique for this report because ICT technologies are where cyber security risks can arise [4, 13, 18, 46, 53]. ICT technologies have become so ubiquitous in almost all sectors, but the level of digitalisation is still different across different sectors. For some sectors, ICT technologies are always used in the context of cyber-physical systems (CPSs), e.g., IoT, WSN, ICS, and SCADA. Table 1 shows an indicative picture of the current level of digitalisation and the use of CPSs across selected NZ-related sectors, based on our personal opinions and understanding of the research literature and real-world systems. Since a precise estimation is impossible nor necessary, we use five broad categorical values: an empty circle (0%, not at all), a circle with a quarter filled (emerging or developing), a half-filled circle (growing, widely used but not everywhere), a circle with three quarters filled (mature, used in a majority of cases), and a full circle (fully developed, ubiquitous use in all cases). We will discuss more about cyber security risks and possible solutions in the next section.

It deserve noting that, scientifically speaking, although ICT technologies map to mainly electronic engineering and computer science and engineering, other disciplines are also actively contributing to development of new ICT technologies and their applications in different domains, e.g., material engineering, mechanical engineering, civil engineering, and chemical and process engineering, automated control and instrument, information systems and operations research, mathematics and statistics, psychology and cognitive sciences. Therefore, research and development on ICT technologies relevant for NZ should be studied taking the inter-disciplinary nature into consideration.

1.2.5 Other Sectors

As shown in Table 1, we also list three other representative NZ-related sectors with a significant GHG emission contribution (business – 18% [39, Section 3.2], residential – 15% [39, Section 3.7], manufacturing – 10.8% [3, Section 1.a], and waste management – 5% [39, Section 3.5], in 2018), all of which are energy consumers and end users of various NZ-related ICT technologies. There are clearly other sectors that should be considered,

© 2022 Crown copyright

Table 1: The level of digitalisation and the use of CPS technologies in some selected NZ-related sectors

Selected Sector	Level of Digitalisation	Use of CPS Technologies
Energy Generation	◔	◔
Energy Networks	◔	◕
Transport & Tourism	◑	◑
Agriculture & Food	◔	◔
Business	◕	◔
Residential	◔	◑
Manufacturing	◔	◑
Waste Management	◔	◔
Telecommunication	◕	●
Digital Services	●	◑

e.g., urban management (for smart cities), healthcare (for smart health), and education, but the way how such sectors are categorised is quite non-standardised, so the sectors listed in Section 1.2 and Table 1 are illustrative rather than comprehensive.

2 Security Risks Associated with NZ-Related Technologies

As mentioned in the previous section, digitalisation has been catalysing the development of NZ-enabling technologies and systems in many sectors, e.g., intelligent transport systems for the transport sector and smart meters for the energy sector. In the mean time, it also increases the attack surface of many physical systems, especially when such systems become accessible remotely from the Internet. The two conflicting aspects suggest that such cyber security risks must be considered carefully to ensure NZ-enabling technologies and systems will work as expected without introducing new vulnerabilities. In addition, due to the use of CPSs in many NZ-related sectors, a successful attack in the cyber world could lead to potential catastrophic consequences in the physical world, such as loss of human lives, damage of physical properties and substantial financial losses [20].

This section gives an overview of different types of cyber security risks we identified through our research, based on our understanding of the literature and our general knowledge about cyber security risks in general. We organise our discussions into two broad categories: technological risks, and socio-technical risks.

2.1 Technological Risks

For this category of cyber security risks, we will first discuss them around some general NZ-enabling ICT technologies, and then in the context of selected NZ technologies in different NZ-related sectors.

© 2022 Crown copyright

2.1.1 Selected General NZ-Enabling Technologies

In 2019, the Royal Society in the UK launched a 'Digital Technology and the Planet' project [47] and produced a report in 2020 to look at the impact of digital technologies on the environment, as well as to identify pathways to use digital technologies for decarbonisation across industries with a set of recommendations [47]. The report indicates that digital technologies alone cannot achieve the NZ goal. However, digital technologies as the enablers can offer promise to catalyse changes to lead to greener ways of living and working. In line with this argument and based on our observations, a number of digital technologies that have been frequently used to help design and develop different NZ-related technologies are identified as representative examples to illustrate associated cyber security risks.

IoT has been widely used to design and develop smart sensing and controlling technologies for many different application domains (e.g., smart cities, intelligent transport systems, smart buildings, smart home, smart health care, ICS and SCADA systems, smart agriculture), many of which can directly or indirectly help reduce GHG emissions. Like many wireless networked systems, the IoT architecture is based on three layers [7]: 1) hardware layer including sensors and actuators with their operation system; 2) communication layer, where the WSNs are used as the main communication technology; and 3) interfaces/services layer which bridges the IoT with end users and other systems served by the IoT. All the three layers of an IoT system can be attacked, and therefore need to be protected against potential malicious attacks. Examples of such cyber security threats include device vulnerabilities, jamming, false data injection, and authentication failures.

AI technologies have attracted a lot of interest from both industry and research communities, thanks to the recent advances of more modern technologies such as deep learning (DL). As already mentioned in Section 1, AI technologies are often used together with IoT technologies to support a wide range of intelligent systems (i.e., almost all the smart systems listed above for the IoT technologies) for NZ purposes. Despite the power of AI technologies, there are cyber security risks associated with them. One particularly relevant one for NZ-related applications is the so-called adversarial AI, where malicious samples are used to make an AI model fail [38], e.g., misleading a road sign detector to cause a car accident. In the NZ context, such failures of AI-based NZ-enabling systems can lead to the opposite effect – increasing GHG emissions rather than reduce them.

Digital twins are digital clones of a physical system, which have found applications in many sectors especially manufacturing, e.g., in smart cities to help simulate and optimise traffic and energy consumption of an ITS. Since digital twins need to communicate with the physical system in real time through network connections, most network-based cyber attacks are possible threats. Digital twins use IoT sensors to get data about the physical system, so all IoT-based cyber security risks exist.

Blockchain technologies have gained popularity recently. By leveraging the concept of a distributed ledger, it can achieve some useful features such as decentralisation, transparency, and pseudonymity. Most blockchain systems are based on proof-of-work (PoW), and computational heavy by design, therefore could be classified as NZ-unfriendly. However, some researchers have proposed to use blockchain technologies for enhancing security of NZ-related systems [19, 25], therefore could be argued an NZ-enabler if their use helps the overall NZ goal of such systems. Independent of the NZ-unfriendliness issue,

© 2022 Crown copyright

there are a wide range of cyber security threats around blockchain technologies, such as privacy concerns, double spending, 51% attacks [21]. We consider the use of blockchain technologies for NZ purposes less mature at this moment and require more research.

Teleconferencing and virtual events have become an everyday reality in all sectors since the global COVID-19 pandemic started in early 2020. In addition to more traditional ICT technologies that support teleconferencing and virtual events, including internet, world wide web, multimedia coding and streaming, software engineering and human-computer interface, more advanced technologies have also been increasingly applied, e.g., AI-based automatic background blurring/replacement and virtual reality (VR) based virtual events. It is no doubt that teleconferencing and virtual events can help reduce GHG emission due to the reduced transport activities and energy use.

2.1.2 NZ-Related Technologies in Selected Sectors

In this sub-subsection, we review some cyber security risks discussed in the research literature, associated with some selected NZ-related technologies used in some specific sectors, mostly based on those listed in Table 1. We also add a few NZ-related technologies with our views on their cyber security risks because we did not notice much related research work. Neither the NZ-technologies nor the cyber security risks discussed here are supposed to be comprehensive, but more used as illustrative examples to show the typical threats one has to consider. It is impossible to use a small report to cover all NZ-related technologies and cyber security risks thoroughly, and we also noticed that related research is very fragmented and insufficient.

- **Energy Generation**
  Marine renewable energy (MRE) systems are designed to provide low-carbon electricity from oceans and rivers for emerging and off-grid markets. de Peralta [15] pointed out some prevalent cyber security risks, including insufficient network boundary protection and poor identification and authentication controls, which can causes damages to business operations, physical assets, digital assets (data stored), and human safety.

- **Energy Networks**

  Demand side management (DSM) in smart grids can handle and analyse electricity load patterns as well as can reshape load profiles to reduce carbon emission. Sarker et al. [40] stated that cyber security and privacy risks are the key challenges for designing and deploying such systems. It is because cyber attackers can launch various attacks such as privacy attacks on users' personal data and manipulation of energy supply information, which can cause serious damages to the society and economy.

  Microgrid integrates local energy production from renewable energy sources, such as hydro, solar, and wind, to provide distributed energy generation and storage, and it is also resilient against power distribution disruption through self-islanding. De Dutta and Prasad [14] listed a number of cyber threats of the microgrid infrastructure, including malicious disconnection of energy sources from the main power

© 2022 Crown copyright

grid and jamming the communication channels. The potential impact could be catastrophic to general public health and safety.

- **Transport & Tourism**

  Intelligent transport systems (ITSs) are part of the development of smart city initiatives to decrease the carbon footprint of the transport sector. An ITS covers many aspects from public transport to private transport. According to Mecheva and Kakanakov [30], different parts of an ITS are vulnerable to different types of cyber security risks such as distributed denial of service (DDoS) attacks, ransomware attacks, relay attacks, wormhole attacks, phishing attacks, and eavesdropping. These cyber attacks could lead to serious physical and economic damages to the society and the general public.

  Internet of vehicles (IoVs) are part of some ITSs, where Internet-enabled vehicles can communicate with each other and exchange data using vehicle-to-vehicle (V2V) protocols. They can help reduce traffic jams and fuel consumption to contribute to NZ emission tasks. Relying on wireless communication can make IoVs vulnerable to jamming and eavesdropping attacks [5].

  Ride-sharing is an technology that can contribute to ease traffic congestion, reduce fuel consumption, and help reducing GHG emission by enabling drivers to share their trips with other riders. As most ride-sharing services are centralised, DDoS can cause a single point of failure and and server hacking can lead to privacy leakage of drivers and riders [6].

  Mobility-as-a-service (MaaS) allows passengers to plan and book multiple transport services from a single interface [54], therefore can help reduce GHG emission via optimising travel efficiency and reducing the use of private cars. Similar to the case of ride-sharing, most MaaS systems are centralised, so the same problems with a single point of failure and privacy concerns exist. Since a MaaS system needs to communicate with multiple transport service providers, there are also cyber risks about unauthorised access to confidential data of some transport service providers by malicious parties (e.g., other service providers and malicious passengers).

  Virtual tourism leverages immersive technologies such as virtual realities (VR) to deliver digital experience of tourism without actually travelling to the real-world sites, which can obviously help reduce GHG emission. A recent piece of research [26] showed its potential during the COVID-19 pandemic and its promising future even after the pandemic is over. Cyber security risks associated with virtual tourism are mostly about the underlying immersive technologies, which include social engineering and privacy leakage caused by unauthorised access [36, 52].

- **Building (Business and Residential)**

  Smart buildings are networks of connected devices and software to manage building functions including lighting, fire alarms, heating, air control, etc. Ciholas et al. [11] pointed out some cyber threats to different layers of a smart building system architecture, such as wireless attacks, DoS attacks, and privacy attacks.

- **Agriculture & Food**

© 2022 Crown copyright

Aquaponic technology is an agricultural production technology combining aquaculture with hydroponics to reduce their combined environment impacts. Taji et al. [44] reviewed aquaponic systems as CPSs utilising IoT and AI technologies, and pointed out that they are susceptible to typical cyber security risks of IoT-based CPSs (see discussions before in Section 2.1.1).

- **Healthcare & Medicine**
  Remote healthcare (also known as telemedicine) has become popular during the COVID-19 pandemic, similar to teleconferencing and virtual events discussed in the previous subsection. There has been positive evidence that telemedicine can indeed help reduce GHG emission greatly [8]. Remote healthcare often makes use of smart sensing and intelligent diagnosis, via the use of ICT technologies such as mobile computing, wearables, IoT, and AI, leading to the concept of **smart healthcare**. Remote and smart healthcare systems are complicated IoE systems including different groups of people and sub-systems, therefore leading to complicated security and privacy risks for different entities [22], which can include loss of human lives, negative impacts on people's health, privacy leakage, legal penalties, and financial losses.

- **Multi-Sector**

  Smart cities are NZ technologies that cover multiple sectors. According to Ma [27], a smart city has four main components: a smart gird, smart buildings, smart transportation, and smart health care. There are other similar definitions where smart buildings are replaced by smart homes Habibzadeh et al. [20]. Hence, the security and privacy landscape for a cross-sector system is more complex and dynamic. As a more complicated system of CPSs, smart cities are vulnerable to all IoT-related attacks discussed in Section 2.1.1, but the attack surface is even larger because of the existence of many system-to-system interfaces.

By looking at the presented NZ-related technologies and systems, it is not hard to notice that many of them are prone to the same or similar cyber security risks. This is because such cyber security risks are more about the underlying ICT enabling technologies rather than the NZ technologies themselves. Considering the complex structure and dynamic nature of NZ-related technologies and systems, the cyber security risk mitigation strategies need to have a holistic approach by considering securing different layers, components and interfaces. Such holistic approaches should not only consider addressing technological risks, but also socio-technical risks, which will be discussed in the next section.

2.2 Socio-Technical Risks

Although there has been some research on technological aspects of cyber security of NZ-related technologies, there seems much less research on socio-technical aspects. During our research, we only noticed very sparse discussions on important socio-technical aspects of cyber security, in the context of NZ-related technologies. In contrast, socio-technical aspects of cyber security have been extensively studied by the cyber security research

© 2022 Crown copyright

community, e.g., as part of the activities of the EPSRC and NCSC-funded Research Institute for Sociotechnical Cyber Security (RISCS) and reflected from multiple knowledge areas of the Cyber Security Body of Knowledge (CyBOK). This lack of research on socio-technical aspects of cyber security for NZ-related technologies is echoed by Habibzadeh et al. [20] in the context of smart cities. They stated that technologies have often developed and deployed quicker than policies and governance mechanisms of cities including information security policies and municipal practices, causing the emergence of a 'security debt'.

In this subsection, considering the lack of research on socio-technical risks of NZ-related technologies in the literature, we list a number of areas policy makers and senior managers should consider, based on our general understanding of research on socio-technical aspects of cyber security in other application domains.

A major aspect to consider is the use of data, which is one of the key components of enabling innovation and technology to help reduce GHGs emissions. However, it poses new challenges that need be addressed not only from technological perspective but also from social perspective such as policy and governance [46]. In the following, we discuss the data perspectives from two areas.

- *Data collection and data use*: Ubiquitous device such as IoT devices and smart phones are frequently used in many 'smart' NZ-related technologies and systems (e.g., smart homes, smart cities). Hence, the data collected can be from a wide range of sources, and the capability of utilising and linking data to generate granular insights such as using location data to derive individual travel patterns, and using smart meter data to deduce individual life/work behaviours, raise the challenge of finding the balance between privacy (e.g., 'how much data need to be collected') and utility (e.g., 'how much information can be derived from the collected data'). Here, the technological objectives of using data-driven approach to optimise NZ-related technologies and systems to improve sustainability is in tension with data security and privacy concerns from individual citizens, therefore requiring systematic considerations, not only in the legal context (e.g., compliance with the UK GDPR and Data Protection Act 2018) and also in the ethical context.

- *Data processing and data storage*: The storage and processing of large amount of data poses another dilemma: centralised vs. decentralised approach. Centralised approaches are often considered easier to manage, and have been widely used in most NZ-related technologies and systems. However, such systems have a single point of failure and can be less resilient in the context of persistent cyber attacks than more decentralised approach. This has led to many efforts of exploring new decentralised and distributed technologies, such as cloud-based storage, blockchain, and federated learning, in order to overcome the problems of centralised approaches. Such decentralised systems are often less computationally efficient so can be considered NZ-unfriendly when used alone, therefore there must be an holistic approach to balance all socio-technical aspects of the whole NZ-related system (e.g., a smart city) to ensure the use of such decentralised technologies will help produce an overall positive sum (i.e., reduction of GHS emission). Such holistic approaches are not simple considering the complexity of many NZ-related systems (e.g., smart cities),

© 2022 Crown copyright

so require consideration of socio-technical aspects such as human psychology, organisational behaviours, legal and economic considerations, among others.

In addition to looking at socio-technical aspects from a data perspective, many other socio-technical perspectives should be carefully considered. Some of such perspectives include information security policies and management of staff competence (e.g., through certification following information security management standards such as ISO/IEC 27000 series[1]); behaviours of different types of human entities (not just users but also designers, developers, policy makers, system administrators, and board members); governance mechanisms across nations, sectors, stakeholders and users; carbon offset and trading platforms where policy leverages and behavioural economics plays a key role; political aspects (e.g., potential mass surveillance of citizens due to the use of NZ-related technologies and systems for environmental monitoring purposes).

When socio-technical aspects have to be considered, the attack surface of NZ-related systems will be substantially increased. Many traditional cyber security risks, such as social engineering, insider threats, cyber fraud, and even cyber conflict between hostile states, will have to be considered. The current ongoing Russia-Ukraine war has witnessed how the NZ goal and the geo-politics can interact to create a potential energy crisis and raised living costs for many countries. As a matter of fact, the mere complexity of socio-technical aspects of cyber security risks mean they are more important than technological ones, which is not surprising since socio-technical risks are broader and include technological risks.

3 Open Challenges

Our research has led to a number of observed open challenges regarding cyber security risks of NZ-related technologies. We briefly summarise some important ones below.

- *The complexity of many NZ-related technologies and systems makes it very challenging to consider cyber security risks holistically.* The nature of the NZ goal requires collaborations of nations, sectors, organisations and citizens, who all have different interests, priorities and levels of cyber security awareness and knowledge. How the whole world can come together to work towards the global NZ goal while managing cyber security risks will not be easy.

- *A lack of a coherent and consistent taxonomy or ontology on NZ-related technologies that can facilitate discussions in different nations, sectors, and communities.* Most research work and technical reports have used different approaches when looking at all NZ-related sectors, technologies and systems. Considering the need of cross-sectoral efforts for the NZ goal, the lack of such a widely accepted (ideally standardised) taxonomy or ontology can harm further collaborations and communications among stakeholders and researchers.

- *An insufficient level of research and consideration on cyber security risks in NZ-related technologies and systems.* Although we noticed some research work that

[1] `https://en.wikipedia.org/wiki/ISO/IEC_27000-series`

© 2022 Crown copyright

explicitly discussed cyber security risks of NZ-related technologies and systems, such discussions are often fragmented and merely echo what have been known in the cyber security community so there are not sufficient contextualisations to the NZ context. In addition, most cyber security discussions on NZ-related technologies and systems so far have focused on technological aspects, but socio-technical aspects deserve more attention due to their importance in large systems of systems (e.g., the concept of IoE).

- *Some NZ-related technologies and systems proposed are NZ-unfriendly when used along, so a more systematic approach to ensure an overall positive sum is required.* We previously used blockchain as a typical example for such NZ-unfriendly technologies that have been proposed to build NZ-enabling systems. Most such proposals have not been critically evaluated, so more research and development is still needed.

4 Recommendations

In this last section, we provide some recommendations to policy makers in both public and private sectors, and also to researchers and solution providers.

- *To strength collaborations between different nations, sectors, stakeholders and communities to have more coordinated efforts on NZ-related activities.* The challenges of considering both technological and socio-technical risks of NZ-related technologies and systems require a more coordinated approach for the global effort. While the UN has been making great efforts in coordinating nation-wide policies and efforts, more cross-sectoral efforts are needed.

- *To develop an NZ-oriented taxonomy and an ontology that consider cyber security risks.* Such a taxonomy and an ontology will greatly help facilitate discussions and collaborations between different nations, sectors, and research communities. This can be done via a piece of contracted research, e.g., as a follow-up project with the authors of this report to extend the incomplete taxonomy we developed for this report.

- *To encourage the NZ research community and the cyber security community work more closely with each other.* These two research communities need to exchange and collaborate with each other more to ensure cyber security risks of NZ-related technologies and systems can be more properly considered and addressed. There are different ways to support such collaboration, such as organising cross-community events, setting up cross-community working groups, and providing funding to encourage researchers from the two communities to work together. One model the UKRI has been using increasingly is to fund a national hub or a Network Plus to support community building and facilitate commissioned research. One example is a £2 million Network Plus for helping "transform foundation industries such as glass, ceramics, paper, metals, bulk chemicals and cement and help the UK meet its ambitious net zero targets" [49].

© 2022 Crown copyright

- *To evaluate the role of NZ-unfriendly and -neutral technologies for achieving the NZ goal more critically.* We need more research and evaluation efforts to ensure the use of NZ-unfriendly and -neutral technologies are fully justified and their ultimate positive role can be evidenced. Setting up testbeds based on technologies such as digital twins could help such critical evaluation.

- *To conduct more systematic literature reviews of cyber security risks of NZ-related technologies and systems.* Our research revealed that a less systematic approach can be limited in its coverage, therefore may lead to biased information that can skew later decisions made. We believe a number of more systematic reviews are necessary, ideally done with a narrow focus, e.g., one review for one more defined sector or type of NZ-related technologies and systems.

- *A number of NZ-enabling virtual or remote technologies deserve further research and development, and new policies supporting their further growth.* Such technologies are very useful for NZ purposes since they can help reduce transport activities. The increasing use of modern ICT techniques such as AI and VR in make such technologies also lead a lot of space for next-generation creative industry, e.g., gaming in metaverse. In this report, we have discussed three example technologies in this group, i.e., teleconferencing and virtual events, virtual tourism, and remote healthcare, but there are clearly many others (e.g., remote learning, e-government) we can consider.

- *The role of ICT technologies in the NZ context requires more research to gain more insights about future best practices.* Due to the special role of ICT technologies (especially the digital parts) and they being the root of cyber security risks, it is important to have a better understanding of their overall role in the NZ context. Although some evidence has shown using ICT technologies can help reduce GHG emission, the over-consumption and increasing use of ICT technologies may also have a negative impact on the NZ goal. We give two typical examples below.

  - *Over use of cyber security mechanisms*: A typical example of such over use is the currently recommended use of SSL/TLS or HTTPS for all websites (i.e., "encryption by default" for all Internet/web traffic), which can lead to unnecessary GHG emission due to avoidable encryption of Internet data that are not sensitive. This is not necessary a small problem, considering the fact that digital videos form over 82% of all web traffic nowadays [2] and the increasing online video consumption can have substainability concerns [17].
  - *Increasing digital duplication*: Although the ubiquitous use of digital technologies has led to a lot of benefits to end users and helped grow the new digital services sector, the existence of so many similar online services have led to a problem of digital duplication – duplicated data and processes across multiple online services and digital systems that lead to "wasted" computations. The rise of decentralised systems such as blockchain makes this worse as the data duplication is pushed to the extreme: a whole distributed ledger is duplicated across all nodes. Policy makers need to have a better understanding about

© 2022 Crown copyright

this phenomenon to know how to refine future policies regulating digital technologies and digital economy. Potential solutions to this digital duplication problem is to develop new data collection and processing frameworks that avoid such duplication by design. Such solutions will require combining both centralised services and more distributed data management closer to the data subjects and streamlined protocols to facilitate communications between data subjects and data consumers. Some relevant technologies include edge and fog computing [55], user-centric data management platforms[2], self-sovereign identity management systems [42], verifiable credentials [43], and MaaS systems we discussed for the transport sector.

Appendixes

A Methodology

The research was conducted following a semi-systematic approach described below.

For the more systematic part, we conducted a systematic search into a major research database, Scopus[3], using a search query with three AND-terms as shown in Table 2. The search was done for meta-data, including title, abstract and keywords fields in Scopus. Since the search itself returned too many items, we limited the results to more recent English papers published in or after 2020, and within the following research disciplines we considered more relevant for NZ technologies: Engineering, Energy, Environment, Computer Science, Mathematics, Social Sciences, Earth Sciences, Agriculture, Business and Decision Sciences, Economics, Physics, Chemistry, Psychology, and Arts. In total, we got 247 returned results, out of which 20 ones have some discussions on cyber security. Those papers were used to inform us about the sectors, NZ technologies, NZ-related systems and ecosystems, cyber security risks and solutions. These papers were not systematically encoded due to the time constraint, but screened and selectively read to allow us to gain an overall picture of a representative subset of related research.

AND-term	Keyword combination(s)
NZ	`"net zero" OR decarboni* OR ((reduc* OR neutral*) AND (carbon OR co2))`
Technologies	`technolog* OR technique*`
Cyber security	`(cyber OR computer OR internet OR network OR online) AND (secur* OR encrypt* OR crypt* OR risk OR attack OR threat OR privacy)`

Table 2: Different AND-terms of the search query we used for identifying relevant research papers.

For the less systematic part, we constructed an informal and high-level taxonomy to

[2]For instance, many recently developed personal data management platforms have such a feature. See `https://mydata.org/organisation-members/` for a list of such MyData operators.

[3]`https://www.scopus.com/`

© 2022 Crown copyright

guide our overall understanding of the whole landscape and our writing of the report. The different categories of NZ-related technologies explained in Section 1.1 and the sector-oriented organisation of the report's content are both based on the taxonomy. Since the taxonomy is still incomplete and less mature, we leave its further development and validation as our future research. In addition to the taxonomy, the report is also heavily based on our personal knowledge and academic judgement, e.g., the level of digitalisation and the use of CPSs in different sectors in Table 1, the discussions on NZ-related technologies and systems that are less investigated in Section 2, and the identified open challenges and recommendations made in the last two sections.

Furthermore, during our research we also conducted ad hoc searches to identify relevant research papers and reports for some specific sectors and NZ-related technologies. Such searches are even less systematic, and we mainly focused on identifying one or two representative recent research papers to illustrate the status of NZ-related sectors and/or cyber security risks of NZ-related technologies.

B Leading Experts in the UK

Based on research papers identified through our quick literature review, we identified a number of UK researchers actively working on NZ technologies. In addition, a number of ongoing research projects funded by the UKRI were identified based on information collected from the websites of UKRI and its relevant research councils, and some highly relevant national research hubs funded by the UKRI, and also based on our personal knowledge. By checking affiliations of all researchers identified, we compiled a number of important research groups and centres that are actively working on NZ-related technologies, and some ongoing research projects focusing on different aspects of NZ-related technologies.

B.1 Research Projects Related to both NZ-Related Technologies and Cyber Security

We identified only two UK research project that studies cyber security risks of NZ-related technologies, both are on cyber security issues of MaaS systems. Considering much more identified projects focusing on NZ technologies and a lot of research projects focusing on different aspects of cyber security and privacy (shown later), the low number of such projects indicates a gap on insufficient ongoing research exploring both topics.

- Mobility as a service: MAnaging Cybersecurity Risks across Consumers, Organisations and Sectors (MACRO), led by Dr Nazmiye Ozkan, Cranfield University; Cyber security part led by Professor Shujun Li
- Increasing User trust in Mobility-as-a-Service IoT ecoSystem (UMIS): co-led by Dr Gary Wills and Professor Tom Cherret, both from the University of Southampton; funded through the PETRAS (see below)

© 2022 Crown copyright

B.2 Some Research Groups and Centres Actively Working on NZ-Related Technologies

- Cardiff University: Cardiff Catalysis Institute
- Cardiff Metropolitan University: Sustainable and Resilient Built Environment (SuRBe) group
- Heriot Watt University: Institute of Chemical Sciences
- Imperial College London: Centre for Environmental Policy, Centre for Energy Policy and Technology, Energy Futures Lab, and Grantham Institute
- London South Bank University: London Centre for Energy Engineering (LCEE
- Loughborough University: Chemical Engineering
- Newcastle University: School of Natural and Environmental Sciences
- Royal Holloway, University of London: Power Systems Group
- Ulster University: Faculty Of Computing, Engineering & Built Environment
- University College London: The Department of Chemistry
- University of Aberdeen: The School of Natural and Computing Sciences
- University of Birmingham: Birmingham Centre for Energy Storage
- University of Bristol: Electrical Energy Management Group
- University of Cambridge: Energy Interdisciplinary Research Centre
- University of Edinburgh: The Institute for Energy Systems
- University of Glasgow: Energy Conversion and Storage
- University of Leeds: School of Earth and Environment
- University of Liverpool: Stephenson Institute for Renewable Energy
- University of Manchester: Manchester Environmental Research Institute
- University of Oxford: Oxford Net Zero and School of Geography and the Environment
- University of Southampton: Waste Management Research Group,
- University of Strathclyde: Future Power Networks and Smart Grids
- University of Surrey: Centre for Sustainability and Wellbeing in the Visitor Economy and Department of Chemical and Process Engineering

© 2022 Crown copyright

B.3 Some Research Projects Related to NZ-Related Technologies

B.3.1 UK Projects

- UK Energy Research Centre (UKERC): led by Professor Robert Gross of Imperial College London, participated by UK researchers from 20 different institutions: Cardiff University, Chatham House, Durham University, Imperial College London, Lancaster University, Newcastle University, Plymouth Marine Laboratory, Science and Technology Facilities Council, University College London, University of Aberdeen, University of Bath, University of East Anglia, University of Edinburgh, University of Exeter, University of Leeds, University of Manchester, University of Oxford, University of Southampton, University of Strathclyde and University of Warwick
- Net-Zero Digital Research Infrastructure Scoping: led by Dr Martin Juckes, Centre for Environmental Data Analysis (CEDA)
- Carbon negative chemicals synthesis directly from the air, led by Dr Melis S. Duyar, University of Surrey
- Decarbonising Nitrogen Fixation for Sustainable Net-Zero Agriculture, led by Dr Mark Symes, University of Glasgow
- Electrocatalysis in non-thermal plasma for energy storage, led by Professor Angel Cuesta Ciscar, University of Aberdeen
- Enabling green ammonia as future transport fuel, led by Dr Xinyan Wang, Brunel University London
- EnergyREV, led by Professor Stephen McArthur, University of Strathclyde
- Energy Superhub Oxford, led by Pivot Power
- "Free-from": transition metal-free and anode-free potassium batteries, led by Dr Yang Xu
- GreenSCIES (Green Smart Community Integrated Energy System), led by Professor Graeme Maidment, London South Bank University
- MIX-MOXes - Mixed Metal Oxides Energy Stations for zero-carbon thermal energy generation with integrated heat storage, led by Dr Adriano Sciacovelli
- Net Zero Geothermal Research for District Infrastructure Engineering (NetZero GeoRDIE), led by Professor David Manning, Newcastle University
- NetworkPlus - A green, connected and prosperous Britain, led by Professor Sandra Dudley-McEvoy, London South Bank University
- Novel Rechargeable Hybrid Redox Flow Battery Based on Particle-Stabilised Emulsions and H2 carriers, led by Professor Marc Pera Titus, Cardiff University

© 2022 Crown copyright

- Port and Coastal Cities and Towns Network, led by Professor William Powrie, University of Southampton
- Project LEO – Local Energy Oxfordshire, led by Stevie Adams, Scottish and Southern Electricity Networks
- Reclaiming Forgotten Cities - Turning cities from vulnerable spaces to healthy places for people [RECLAIM], led by Professor Sandra Dudley-McEvoy, London South Bank University
- Responsive Flexibility (ReFLEX), led by European Marine Energy Centre (EMEC)
- Sustainable Catalysis for Clean Growth, led by Professor Duncan Wass
- Sustainable Hydrogen Production from Seawater Electrolysis, led by Professor Wen-Feng Lin, Loughborough University
- The Supergen Energy Networks Hub, led by Professor Phil Taylor, Bristol University
- Transformative Recovery of Low-Grade Waste Heat using Ionic Thermoelectrics, led by Dr Jan-Willem Bos, Heriot-Watt University
- Zero-Chem: Zerogap bipolar membrane electrolyser for CO2 reduction to chemicals & fuels, led by Professor Alexander Cowan, University of Liverpool

B.3.2 European Projects Participated by UK Researchers

- Constraining uncertainty of multi decadal climate projections (CONSTRAIN), led by Professor Piers Forster, University of Leeds; participated by Dr Joeri Rogelj, Imperial College London
- Collaborative development of renewable/thermally driven and storage-integrated cooling technologies (CO-COOL), led by Professor Yongliang Li
- Quantifying and Deploying Responsible Negative Emissions in Climate Resilient Pathways (NEGEM), participated by Energy Interdisciplinary Research Centre, University of Cambridge, Professor Myles Allen, University of Oxford, and Professor Niall Mac Dowell, Imperial College London
- Carbon Risk Real Estate Monitor (CRREM, participated by Professor Martin Haran, Ulster University
- Pan-European system with an efficient coordinated use of flexibilities for the integration of a large share of RES (EU-SysFlex), participated by Dr Damian Flynn, University College Dublin and Professor Goran Strbac, Imperial College London
- Fast-tracking Offshore Renewable energy With Advanced Research to Deploy 203,0MW of tidal energy before 2030 (FORWARD-2030), participated by The Institute of Energy System, University of Edinburgh

© 2022 Crown copyright

B.4 Selected Research Centres and Projects Related to Cyber Security

There are a large number of research centres and projects in the UK that focus on different cyber security topics. For NZ-related technologies, the following three national (cross-institutional) research hubs are of particular interest due to their focus on cyber security and trust aspects of IoT, CPSs and autonomous systems.

- Research Institute in Trustworthy Interconnected Cyber-physical Systems (RITICS): co-led by Professor Chris Hankin and Professor Deeph Chana of the Imperial College London; participated by many UK researchers from the University of Birmingham; University of Bristol; Brunel University; Cardiff University; City, University of London; University of Coventry; De Montfort University; University of Glasgow; University of Hudderfield; University of Kent; King's College University; Lancaster University; University of Manchester; University of Oxford; Queen's University Belfast; Royal Holloway, University of London; University of Sheffield; University of Southampton; University College London; and University of Warwick.

- PETRAS (Privacy, Ethics, Trust, Reliability, Acceptablity and Security) National Centre of Excellence on IoT devices, systems and networks: led by Professor Jeremy Watson from the University College London (UCL); participated by researchers from 21 UK universities – UCL; Imperial College London; University of Oxford; Lancaster University; University of Warwick; University of Southampton; Newcastle University; University of Nottingham; University of Bristol; Cardiff University; University of Edinburgh; University of Surrey; Coventry University; Northumbria University; University of Glasgow; Cranfield University; De Montfort University; Durham University; University of Manchester; Royal Holloway, University of London; and University of Strathclyde.

- UKRI Trustworthy Autonomous Systems (TAS) Hub: led by Professor Sarvapali D. (Gopal) Ramchurn from the University of Southampton; co-led by a group of UK researchers from University of Southampton, University of Nottingham and King's College London.

The above three national research hubs have all been funding research projects conducted by UK researchers from more universities. While we did not notice any ongoing or new projects focus particularly on NZ-related technologies, some have good connections with NZ-related technologies. We list some selected ones below:

- Interconnected Safe and Secure Systems (IS3): led by Dr Peter Popov, City, University of London; funded through the RITICS

- NDN for Secure Industrial IoT Networking: led by Professor Awais Rashid, University of Bristol; funded through the RITICS

- DigiPort: From Logistics 4.0 to Digital Ports: A study in transformability using DLTs: led by Professor Julie McCann, Imperial College London; funded through the PETRAS

© 2022 Crown copyright

- SDRIOTSS (Software Defined Receiver IoT Spectrum Survey) 2: led by Dr Matthew Ritchie, University College London; funded through the PETRAS
- Intersectional Approaches to Design and Deployment of Trustworthy Autonomous Systems: led by Dr Caitlin Bentley, University of Sheffield; funded through the TAS Hub
- Trust Assurance in Autonomous Cyber-Physical Agriculture Farms of Future (AgriTrust): led by Dr Shishir Nagaraja, University of Strathclyde; funded through the TAS Hub

C Some Relevant Journals and Magazines

During the research work we also identified a number of scientific journals and magazines closely related to NZ technologies, which we list below. We also include several major journals and magazines that focus on cyber security as they often publish papers on cyber security risks of NZ-related technologies. Note that this list is not comprehensive and for cyber security conferences are also very important, so we recommend considering a more systematic approach to extend this list.

C.1 NZ-Related Journals and Magazines

- Energy Policy, since 1973, published by the Elsevier B.V.
- Journal of Industrial Ecology: since 1997, published by the International Society for Industrial Ecology
- Renewable and Sustainable Energy Reviews: since 1997, published by the Elsevier B.V.
- International Journal of Low-Carbon Technologies: since 2006, published by the Oxford University Press
- Energy & Environmental Science: since 2008 published by the Royal Society of Chemistry
- Nature Climate Change: since 2011, published by the Springer Nature Limited
- Sustainable Cities and Society: since 2011, published by the Elsevier B.V.
- Nature Energy: since 2016, published by the Springer Nature Limited
- Nature Sustainability: since 2016, published by the Springer Nature Limited
- IEEE Transactions on Sustainable Computing: since 2016, published by the IEEE
- IEEE Transactions on Green Communications and Networking: since 2017, published by the IEEE
- IEEE Transactions on Intelligent Transportation Systems: since 2000, published by the IEEE

© 2022 Crown copyright

- Renewable Energy: since 2003, published by the Elsevier B.V.
- IEEE Intelligent Transportation Systems Magazine: since 2009, published by the IEEE
- IEEE Transactions on Smart Grid: since 2010, published by the IEEE
- IEEE Transactions on Sustainable Energy: since 2010, published by the IEEE
- IET Renewable Power Generation: since 2013, published by the IET
- IEEE Transactions on Transportation Electrification: since 2015, published by the IEEE
- IEEE Transactions on Intelligent Vehicles: since 2016, published by the IEEE
- Current Opinion in Green and Sustainable Chemistry: since 2016, published by the Elsevier B.V.
- IEEE Open Journal of Intelligent Transportation Systems: since 2020, published by the IEEE
- Energy Research and Social Science: since 2014, published by the Elsevier B.V.

C.2 Cyber Security-Related Journals and Magazines

- ACM Transactions on Privacy and Security (formerly known as ACM Transactions on Information and System Security): since 2003, published by the ACM
- IEEE Security & Privacy: since 2003, published by the IEEE
- IEEE Transactions on Dependable and Secure Computing: since 2004, published by the IEEE
- Computers & Security: since 1982, published by the Elsevier B.V.
- Journal of Computer Security: since 1992, published by the IOS Press
- IET Information Security: since 2007, published by the IET
- International Journal of Critical Infrastructure Protection: since 2008, published by the Elsevier B.V.
- Digital Threats: Research and Practice: since 2020, published by the ACM

© 2022 Crown copyright

References

[1] [n.d.]. IRENA – International Renewable Energy Agency. Website. https://www.irena.org/

[2] 2018. *VNI Complete Forecast Highlights*. Technical Report. Cisco. https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_Device_Growth_Traffic_Profiles.pdf

[3] 2020. *The Sixth Carbon Budget: Manufacturing and construction*. Technical Report. Climate Change Committee. https://www.theccc.org.uk/wp-content/uploads/2020/12/Sector-summary-Manufacturing-and-construction.pdf

[4] Maria Antikainen, Teuvo Uusitalo, and Päivi Kivikytö-Reponen. 2018. Digitalisation as an Enabler of Circular Economy. *Procedia CIRP* 73 (2018), 45–49. https://doi.org/10.1016/j.procir.2018.04.027 10th CIRP Conference on Industrial Product-Service Systems, IPS^2 2018, 29-31 May 2018, Linköping, Sweden.

[5] Chandra Bajracharya. 2021. Performance Evaluation for Secure Communications in Mobile Internet of Vehicles With Joint Reactive Jamming and Eavesdropping Attacks. *IEEE Transactions on Intelligent Transportation Systems* (2021), 8 pages. https://doi.org/10.1109/TITS.2021.3095015

[6] Mohamed Baza, Mohamed Mahmoud, Gautam Srivastava, Waleed Alasmary, and Mohamed Younis. 2020. A Light Blockchain-Powered Privacy-Preserving Organization Scheme for Ride Sharing Services. In *Proceeding of the 2020 IEEE 91st Vehicular Technology Conference*. IEEE, 6 pages. https://doi.org/10.1109/VTC2020-Spring48590.2020.9129197

[7] Mardiana Binti and Wan Haslina Hassan. 2019. Current research on Internet of Things (IoT) security: A survey. *Computer Networks* 148 (2019), 283–294. https://doi.org/10.1016/j.comnet.2018.11.025

[8] Stephen Blenkinsop, Aideen Foley, Natascha Schneider, Joseph Willis, Hayley J. Fowler, and Sanjay M. Sisodiya. 2021. Carbon emission savings and short-term health care impacts from telemedicine: An evaluation in epilepsy. *Epilepsia* 62, 11 (2021), 2732–2740. https://doi.org/10.1111/epi.17046

[9] Stéphanie Bouckaert, Araceli Fernandez Pales, Christophe McGlade, Uwe Remme, Brent Wanner, Laszlo Varro, Davide D'Ambrosio, Thomas Spencer, et al. 2021. *Net Zero by 2050: A Roadmap for the Global Energy Sector*. Special Report. International Energy Agency (IEA). https://www.iea.org/reports/net-zero-by-2050

[10] Modassar Chaudry, Lahiru Jayasuriya, and Nick Jenkins. 2021. Modelling of integrated local energy systems: Low-carbon energy supply strategies for the Oxford-Cambridge arc region. *Energy Policy* 157, Article 112474 (2021), 22 pages. https://doi.org/10.1016/j.enpol.2021.112474

© 2022 Crown copyright

[11] Pierre Ciholas, Aidan Lennie, Parvin Sadigova, and Jose M. Such. 2019. The Security of Smart Buildings: a Systematic Literature Review. arXiv:1901.05837 [cs.CR]. https://doi.org/10.48550/arXiv.1901.05837

[12] European Commission. 2016. A European Strategy for Low-Emission Mobility. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committeee and the Committee of the Regions. https://www.eea.europa.eu/policy-documents/a-european-strategy-for-low

[13] Sneha Dawda, Chamin Herath, and Jamie MacColl. 2022. *Securing a Net-Zero Future: Cyber Risks to the Energy Transition*. Emerging Insights. Royal United Services Institute (RUSI). https://rusi.org/explore-our-research/publications/emerging-insights/securing-net-zero-future-cyber-risks-energy-transition

[14] Sarmistha De Dutta and Ramjee Prasad. 2020. Cybersecurity for Microgrid. In *Proceeding of the 2020 23rd International Symposium on Wireless Personal Multimedia Communications*. IEEE, 5 pages. https://doi.org/10.1109/WPMC50192.2020.9309494

[15] Fleurdeliza A. de Peralta. 2020. Cybersecurity Resiliency of Marine Renewable Energy Systems-Part 1: Identifying Cybersecurity Vulnerabilities and Determining Risk. *Marine Technology Society Journal* 54, 6 (2020), 97–107. https://doi.org/10.4031/MTSJ.54.6.9

[16] G. Dileep. 2020. A survey on smart grid technologies and applications. *Renewable Energy* 146 (2020), 2589–2625. https://doi.org/10.1016/j.renene.2019.08.092

[17] Chris Evans, Julian Issa, and Simon Forrest. 2020. *The Sustainable Future of Video Entertainment: From creation to consumption*. Technical Report. Futuresource Consulting Ltd. https://www.interdigital.com/download/5fc4ff868934bf7f7ae2534d

[18] Rebecca Ford and Jeffrey Hardy. 2020. Are we seeing clearly? The need for aligned vision and supporting strategies to deliver net-zero electricity systems. *Energy Policy* 147, Article 111902 (2020), 12 pages. https://doi.org/10.1016/j.enpol.2020.111902

[19] Keke Gai, Yulu Wu, Liehuang Zhu, Meikang Qiu, and Meng Shen. 2019. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. *IEEE Transactions on Industrial Informatics* 15, 6 (2019), 3548–3558. https://doi.org/10.1109/TII.2019.2893433

[20] Hadi Habibzadeh, Brian H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata. 2019. A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities. *Sustainable Cities and Society* 50 (2019), 20 pages. https://doi.org/10.1016/J.SCS.2019.101660

© 2022 Crown copyright

[21] Huru Hasanova, Ui-jun Baek, Mu-gon Shin, Kyunghee Cho, and Myung-Sup Kim. 2019. A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures. *International Journal of Network Management* 29, 2 (2019). https://doi.org/10.1002/nem.2060

[22] Sivanarayani M. Karunarathne, Neetesh Saxena, and Muhammad Khurram Khan. 2021. Security and Privacy in IoT Smart Healthcare. *IEEE Internet Computing* 25, 4 (2021), 37–48. https://doi.org/10.1109/MIC.2021.3051675

[23] David J. Langley, Jenny van Doorn, Irene C. L. Ng, Stefan Stieglitz, Alexander Lazovik, and Albert Boonstra. 2021. The Internet of Everything: Smart things and their impact on business models. *Journal of Business Research* 122 (2021), 853–863. https://doi.org/10.1016/j.jbusres.2019.12.035

[24] Manfred Lenzen, Ya-Yen Sun, Futu Faturay, Yuan-Peng Ting, Arne Geschke, and Arunima Malik. 2018. The carbon footprint of global tourism. *Nature Climate Change* 8 (2018), 522–528. https://doi.org/10.1038/s41558-018-0141-x

[25] Tong Liu, Fariza Sabrina, Julian Jang-Jaccard, Wen Xu, and Yuanyuan Wei. 2022. Artificial Intelligence-Enabled DDoS Detection for Blockchain-Based Smart Transport Systems. *Sensors* 22, 1, Article 32 (2022), 22 pages. https://doi.org/10.3390/s22010032

[26] Junyu Lu, Xiao Xiao, Zixuan Xu, Chenqi Wang, Meixuan Zhang, and Yang Zhou. 2022. The potential of virtual tourism in the recovery of tourism industry during the COVID-19 pandemic. *Current Issues in Tourism* 25, 3 (2022), 441–457. https://doi.org/10.1080/13683500.2021.1959526

[27] Chen Ma. 2021. Smart City and Cyber-security: Technologies Used, Leading Challenges and Future Recommendations. *Energy Reports* 7 (2021), 7999–8012. https://doi.org/10.1016/J.EGYR.2021.08.124

[28] Jens Malmodin, Dag Lundén, øAsa Moberg, Greger Andersson, and Mikael Nilsson. 2014. Life Cycle Assessment of ICT. *Journal of Industrial Ecology* 18, 6 (2014), 829–845. https://doi.org/10.1111/jiec.12145

[29] Valérie Masson-Delmotte, Panmao Zhai, Hans-Otto Pörtner, Debra Roberts, Jim Skea, Priyadarshi R. Shukla, Anna Pirani, W. Moufouma-Okia, C. Péan, R. Pidcock, Sarah Connors, J. B. Robin Matthews, Yang Chen, X. Zhou, M. I. Gomis, E. Lonnoy, T. Maycock, M. Tignor, and T. Waterfield. 2018. *Global warming of 1.5°C. An IPCC Special Report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development and efforts to eradicate poverty.* Special Report SR15. IPCC (Intergovernmental Panel on Climate Change). https://www.ipcc.ch/sr15/

[30] Teodora Mecheva and Nikolay Kakanakov. 2020. Cybersecurity in Intelligent Transportation Systems. *Computers* 9, 4, Article 83 (2020), 12 pages. https://doi.org/10.3390/computers9040083

© 2022 Crown copyright

[31] Seymour Millen and Ellie Page. 2013. *Emissions due to agriculture: Global, regional and country trends 2000–2018*. Technical Report FAOSTAT Analytical Brief 18. Food and Agriculture Organization of the United Nations. https://www.fao.org/3/cb3808en/cb3808en.pdf

[32] Seymour Millen and Ellie Page. 2013. *Tackling Climate Change through Livestock: A global assessment of emissions and mitigation opportunities*. Technical Report. Food and Agriculture Organization of the United Nations. https://www.fao.org/3/i3437e/i3437e00.htm

[33] Seymour Millen and Ellie Page. 2020. *Farming for Failure*. Technical Report. Greenpeace. https://storage.googleapis.com/planet4-eu-unit-stateless/2020/09/20200922-Greenpeace-report-Farming-for-Failure.pdf

[34] Seymour Millen and Ellie Page. 2021. *Transport and Environment Statistics: 2021 Annual report*. Governmental Report. Department for Transport (UK). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/984685/transport-and-environment-statistics-2021.pdf

[35] Francesco Nocito and Angela Dibenedetto. 2020. Atmospheric CO2 mitigation technologies: carbon capture utilization and storage. *Current Opinion in Green and Sustainable Chemistry* 21 (2020), 34–43. https://doi.org/10.1016/j.cogsc.2019.10.002

[36] Nasreen Parvez. 2022. What does metaverse cybersecurity mean and imply? Web page. https://www.smarcil.com/what-does-metaverse-cybersecurity-mean-and-imply/

[37] Claudia Rahmann and Ricardo Alvarez. 2022. The Role of Smart Grids in the Low Carbon Emission Problem. In *Planning and Operation of Active Distribution Networks*. Lecture Notes in Electrical Engineering, Vol. 826. Springer, 455–485. https://doi.org/10.1007/978-3-030-90812-6_17

[38] Kui Ren, Tianhang Zheng, Zhan Qin, and Xue Liu. 2020. Adversarial Attacks and Defenses in Deep Learning. *Engineering* 6, 3 (2020), 346–360. https://doi.org/10.1016/j.eng.2019.12.012

[39] Ricardo Energy & Environment. 2020. *Sector, Gas, and Uncertainty Summary Factsheets - Greenhouse Gas Emissions*. Technical Report. Department for Business, Energy & Industrial Strategy (UK). https://naei.beis.gov.uk/resources/Sector_Summary_Factsheet_2020-v2.html

[40] Eity Sarker, Pobitra Halder, Mehdi Seyedmahmoudian, Elmira Jamei, Ben Horan, Saad Mekhilef, and Alex Stojcevski. 2021. Progress on the demand side management in smart grid and optimization approaches. *International Journal of Energy Research* 45, 1 (2021), 36–64. https://doi.org/10.1002/er.5631

[41] Scottish Government. 2020. Reducing Greenhouse Gas Emissions. Web page. https://www.gov.scot/policies/climate-change/reducing-emissions/

© 2022 Crown copyright

[42] Reza Soltani, Uyen Trang Nguyen, and Aijun An. 2021. A Survey of Self-Sovereign Identity Ecosystem. *Security and Communication Networks* 2021, Article 8873429 (2021), 26 pages. https://doi.org/10.1155/2021/8873429

[43] Manu Sporny, Dave Longley, and David Chadwick. 2022. *Verifiable Credentials Data Model v1.1.* W3C Recommendation. W3C. https://www.w3.org/TR/vc-data-model/

[44] Khaoula Taji, Rachida Ait Abdelouahid, Ibtissame Ezzahoui, and Abdelaziz Marzak. 2021. Review on architectures of aquaponic systems based on the Internet of Things and artificial intelligence: Comparative study. In *Proceedings of the 2021 4th International Conference on Networking, Information Systems & Security*. ACM, Article 50, 9 pages. https://doi.org/10.1145/3454127.3457625

[45] P. C. Taylor, M. Abeysekera, Y. Bian, D. Ćetenović, M. Deakin, A. Ehsan, V. Levi, F. Li, R. Oduro, R. Preece, P. G. Taylor, V. Terzija, S. L. Walker, and J. Wu. 2022. An interdisciplinary research perspective on the future of multi-vector energy networks. *International Journal of Electrical Power & Energy Systems* 135, Article 107492 (2022), 14 pages. https://doi.org/10.1016/j.ijepes.2021.107492

[46] The Royal Society. 2019. *Digital technologies and human transformations*. Workshop report. The Royal Society. https://royalsociety.org/topics-policy/publications/2020/digital-technologies-and-human-transformations/

[47] The Royal Society. 2020. *Digital technology and the planet: Harnessing computing to achieve net zero*. Technical report. https://royalsociety.org/topics-policy/projects/digital-technology-and-the-planet/

[48] UK Government. 2019. UK Becomes First Major Economy to Pass Net Zero Emissions Law. News release. https://www.gov.uk/government/news/uk-becomes-first-major-economy-to-pass-net-zero-emissions-law

[49] UK Research and Innovation (UKRI). 2020. UKRI awards £2 million Network Plus grant. News release. https://www.ukri.org/news/ukri-awards-2-million-network-plus-grant/

[50] United Nations. 2021. COP26: Together for Our Planet. Web page. https://www.un.org/en/climatechange/cop26

[51] United Nations, UN Climate Change Conference UK 2021, and UK Government. 2021. *COP26: The Glasgow Climate Pact*. Technical Report. https://ukcop26.org/wp-content/uploads/2021/11/COP26-Presidency-Outcomes-The-Climate-Pact.pdf

[52] Karthik Viswanathan and Abbas Yazdinejad. 2022. Security Considerations for Virtual Reality Systems. arXiv:2201.02563 [cs.CR]. https://doi.org/10.48550/arXiv.2201.02563

© 2022 Crown copyright

[53] Eric Ke Wang, Yunming Ye, Xiaofei Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow. 2010. Security Issues and Challenges for Cyber Physical System. In *Proceeding of the 2010 IEEE/ACM International Conference on Green Computing and Communications and International Conference on Cyber, Physical and Social Computing*. IEEE, 733–738. https://doi.org/10.1109/GreenCom-CPSCom.2010.36

[54] Yale Z. Wong, David A. Hensher, and Corinne Mulley. 2020. Mobility as a service (MaaS): Charting a future context. *Transportation Research Part A: Policy and Practice* 131 (2020), 5–19. https://doi.org/10.1016/j.tra.2019.09.030

[55] Ashkan Yousefpour, Caleb Fung, Tam Nguyen, Krishna Kadiyala, Fatemeh Jalali, Amirreza Niakanlahiji, Jian Kong, and Jason P. Jue. 2019. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture* 98 (2019), 289–330. https://doi.org/10.1016/j.sysarc.2019.02.009

[56] Zhien Zhang, Tao Wang, Martin J. Blunt, Edward John Anthony, Ah-Hyung Alissa Park, Robin W. Hughes, Paul A. Webley, and Jinyue Yan. 2020. Advances in carbon capture, utilization and storage. *Applied Energy* 278, Article 115627 (2020), 3 pages. https://doi.org/10.1016/j.apenergy.2020.115627

© 2022 Crown copyright