RUSI
Royal United Services Institute
for Defence and Security Studies

EMERGING INSIGHTS

Securing a Net-Zero Future

Cyber Risks to the Energy Transition

Sneha Dawda, Chamin Herath and Jamie MacColl

JANUARY 2022

EXECUTIVE SUMMARY

Climate change is the biggest threat to modern society. Our reliance on fossil fuels for energy production has caused large-scale emissions of harmful greenhouse gases, such as CO2, which is causing the global temperature to rise at an alarming rate. Research has highlighted that the only way to slow down its effects and control the global temperature is to reach net-zero greenhouse gas emissions as fast as possible. A key component of this is shifting to a low-carbon energy system where renewable sources are used to produce electricity which can be used for power, heat and transport. As a result, UK investment in the transition to renewable electricity infrastructure over the next decade and beyond is inevitable.

Yet, as an area of critical importance, energy systems are often the target of malicious cyber attacks. As we make the shift towards renewables, there will be a greater reliance on smart electricity systems which must be resilient to these types of attacks. In this regard, this Emerging Insights paper examines the cyber risk to the UK's energy transition by focusing on renewable electricity infrastructure. The future low-carbon energy system will consist of a wide range of energy production, but a full examination of these sources is outside the scope of this paper. While research has often examined the cyber risk to low-carbon non-renewables such as nuclear power, less attention has been paid to understanding the cyber risk to renewables.

Though research on this subject is growing, it remains largely technical, making it less accessible for policymakers and the wider public. Furthermore, research is largely based on a US context, with less attention paid to the UK and its changing energy infrastructure. Using findings from existing literature and insights derived from a consultative workshop with subject matter experts, this paper identifies six key risks to renewable electricity production and distribution, storage, and consumer and business energy management technology:

Risk 1: Vulnerabilities in supervisory control and data acquisition (SCADA) systems. Insecure communication channels between SCADA and different parts of the distributed renewable electricity system, remote access and increased automation.

Risk 2: Legacy technology. Outdated and insecure grid infrastructure.

Risk 3: Supply chains. Long and complex global technology supply chains and poor supply chain risk mitigation strategies.

Risk 4: Lithium-ion batteries. Weaknesses in encryption, authorisation and remote access in battery management systems (BMS).

Risk 5: Home car chargers and consumer touchpoints. Vulnerabilities in firmware and a lack of industry standards.

Risk 6: Smart home and building 'Internet of Things' (IoT). A large attack surface from a vast number of IoT devices with physical and remote access points.

While the cyber risks identified in this paper are not entirely new, its main contribution is to present a top-level overview of the key challenges that will impact the reliability and safety of the future electricity sector in the UK. Beyond identifying these risks, this paper highlights key policy questions around the risk mitigation of the sector. In doing so, it calls for further research into risk mitigation strategies and policy-focused recommendations on securing the UK's net-zero future.

INTRODUCTION

Renewable electricity will be a policy priority for governments for the foreseeable future. A recent IPCC report warned governments that the Earth is on track to reach over 1.5 degrees Celsius of warming and that climate change has reached a point of no return.[1] The future of climate change, the report said, is dependent on how quickly humans stop relying on fossil fuels and carbon-intensive industries. This was a key point of discussion in the recent UN Climate Change Conference, COP26, with world leaders emphasising the need to fast-track the widespread adoption of clean energy technologies.[2]

Cyber threats to energy infrastructure are becoming more ubiquitous.[3] As a result, a priority of the energy transition should be ensuring the reliability and safety of renewable electricity and other low-carbon technologies.[4] As these technologies are becoming smarter and more connected, the renewable electricity system will need a common understanding of cyber threats and mitigation strategies.[5] This paper sets out some of the cyber risks the sector could face and calls for UK-based research into risk mitigation strategies.

1. IPCC, 'Summary for Policymakers', 2019, p. 5, <https://www.ipcc.ch/site/assets/uploads/sites/2/2019/05/SR15_SPM_version_report_LR.pdf>, accessed 29 November 2021.
2. COP26, <https://ukcop26.org/>, accessed 29 November 2021; Roger Harrabin, 'COP26: Leaders Agree Global Plan to Boost Green Technology', *BBC News*, 2 November 2021.
3. Phil Muncaster, 'Wind Turbine Giant Offline After Cyber Incident', *InfoSecurity*, 22 November 2021; Zach Marzouk, 'South Australia Government Data Breached in Ransomware Attack', ITPro, 10 December 2021.
4. Distributed energy systems are defined as containing a wide range of energy production, distribution, storage and monitoring methods. For more information, see Siemens, 'Be Energy Intelligent – With Distributed Energy Solutions', <https://new.siemens.com/global/en/products/energy/topics/distributed-energy-systems.html>, accessed 16 August 2021.
5. Nick Ferris and Sonja van Renssen, 'Cybersecurity Threats Escalate in the Energy Sector', Energy Monitor, 17 February 2021, <https://energymonitor.ai/tech/

Over the last decade, the UK has been increasing investment and installation of renewable electricity sources. Alongside several other countries, the UK government initially committed to becoming a net-zero country by 2050. This will require massive transformation of infrastructure and unavoidable changes to society.[6] Yet, evidence around how quickly the climate is changing has called the length of this timeline – and other countries' timelines – into question and a new target has been set for net zero by 2035. However, a faster transition could lead to increased cyber risk. To meet demand, infrastructure will need to be built at pace and at cheaper cost, which may result in the use of potentially less reliable technology built by a global supply chain with varying standards. Therefore, any shift to new infrastructure must happen with cyber resilience front and centre for society to safely reap the benefits. There is a role for government in ensuring infrastructure is built with appropriate standards and with cyber risk mitigation as a priority.

Any shift to new infrastructure must happen with cyber resilience front and centre for society to safely reap the benefits

The energy sector enables all other critical infrastructure – and society itself – to function. Future renewable electricity sources must be built on cyber-resilient infrastructure, with an end-to-end risk management strategy. This paper seeks to understand current cyber-related risks to renewable electricity production, distribution, storage and consumer energy management technologies. Some of the risks reflect those experienced by the fossil fuel industry, including information technology (IT) and operational technology (OT) convergence, legacy industrial control systems (ICS), and supply chain risks.[7] However, other risks are novel to the renewable electricity sector and the digitalisation that has come with renewables, such as lithium-ion batteries and a rapidly increasing consumer technology environment.

Digitalisation opens opportunities, from more accurate energy distribution in line with weather patterns to sensors on hardware that can predict

digitalisation/cybersecurity-threats-escalate-in-the-energy-sector>, accessed 16 August 2021; Michael Ruhle and Lukas Trakimavicius, 'Cyberattacks Are the New Challenge for Renewable Energy', *Politico*, 18 July 2017.

6. Nadeem Badshah, 'UK's Net Zero Goal "Too Far Away", Says No 10 Climate Spokesperson', *The Guardian*, 1 August 2021; National Infrastructure Commission, 'Net-Zero: Commission Recommendations and the Net Zero Target', May 2020, <https://nic.org.uk/app/uploads/Net-Zero-Report-May-2020.pdf>, accessed 16 August 2021; Institution of Civil Engineers (ICE), 'A Plan for Transitioning Infrastructure to Net Zero: The Policy Choices', September 2020, <https://www.ice.org.uk/getattachment/news-and-insight/policy/plan-for-transitioning-infrastructure-to-net-zero/ICE_Net-Zero_Infrastructure_Plan_Paper__Final.pdf.aspx#_ga=2.102623553.1168195173.1632820072-280043737.1632820072>, accessed 16 August 2021.
7. In accordance with NIST, Industrial Control Systems (ICS) can be defined as 'an information system used to control industrial processes such as manufacturing, product handling, production, and distribution'. They are used in various critical sectors such as energy and water. See NIST, 'ICS', <https://csrc.nist.gov/glossary/term/ICS>, accessed 29 November 2021.

and prevent major breakage and disruption.[8] However, with increased technology, there is increased cyber risk. It is paramount that renewable technology is supported with appropriate risk management. This paper seeks to prompt a discussion around risk management of renewables from the micro (such as the solar panels on a house) to the macro level (such as large offshore wind farms).

METHODOLOGY AND STRUCTURE

This paper is part of a series published under RUSI's 'Globalisation of Technology' research project,[9] which aims to explore the cyber security risks from the growing presence of foreign-made components in current and emerging technologies. In doing so, it seeks to disentangle the political, economic and technical factors that inform policy choices across various critical sectors. In a 2020 paper, the project explored the cyber risks to the 5G telecommunications sector.[10]

This paper is based on two main sources of data. First, research involved a literature review of publicly available academic journal articles, book chapters, and 'grey literature' such as industry and government reports from 2014 to 2021. All pieces of literature were identified between March and December 2021 through Google Scholar and EBSCO. A series of keyword search strings were used to identify relevant literature and additional sources were identified through snowballing.[11]

Second, a consultative workshop was held on 10 March 2021 with 22 subject matter experts from 15 different organisations across government, the private sector and civil society. It took place under the Chatham House Rule.[12] Data collection was based on three key questions:

1. Which parts of the energy sector are at risk and why?

2. What types of emerging technology will disrupt the electricity sector over the next decade and what will the cyber security implications be?

3. Where are the greatest cyber risks in the vendor supply chain and how are they currently managed?

---

8. Aidan Rhodes, 'Digitalisation of Energy: An Energy Futures Lab Briefing Paper', Imperial College London, May 2020.
9. See RUSI, 'Globalisation of Technology', <https://rusi.org/explore-our-research/projects/globalisation-technology>.
10. James Sullivan and Rebecca Lucas, '5G Cyber Security: A Risk-Management Approach', *RUSI Occasional Papers* (February 2020).
11. 'Snowballing' is a form of literature search that helps identify additional sources from the literature already identified.
12. Chatham House, 'Chatham House Rule', <https://www.chathamhouse.org/about-us/chatham-house-rule>, accessed 29 November 2021.

To address the cyber risks to the UK's renewable electricity sector, this paper is divided into two sections. The first section outlines the renewable electricity sector within the UK context. It defines different types of renewable electricity, the UK stakeholder ecosystem and policy landscape that manages cyber risk, the digitalisation of the electricity sector and distributed energy systems, and the cyber threat to renewables. The second section identifies six key cyber risks which cover three core areas of the renewable electricity system: energy production and distribution; energy storage; and consumer and business energy management technology. While this paper aims to provide a broad overview of the six risks it identifies, evidence-driven recommendations for policy and an in-depth assessment of how they can be effectively managed are beyond its scope.

THE UK'S RENEWABLE ELECTRICITY SECTOR

This section outlines the UK's renewable electricity sector. It defines different types of renewables and summarises the stakeholders and policies involved in the transition to renewable technology. Following this, it describes the key components involved in the digitalisation of energy systems and outlines the cyber threat to the renewable electricity sector.

The percentage of energy produced by renewables has grown substantially over the last decade. Global renewable electricity capacity grew by 45% between 2019 to 2020, mainly due to a 90% rise in wind capacity.[13] The International Energy Agency estimated there would be an 8% increase in renewable energy generation in 2021, and global renewable electricity capacity is set to grow by 60% in the next five years.[14] The UK is deeply invested in renewables, with 43% of its electricity generation coming from renewable sources in 2020.[15] Together, wind and solar power accounted for 29% of the UK's total electricity generation. This is more than three times the global average and just over double the amount it was producing five years ago.[16] Although the UK's energy generation through renewables has slowed due to a lack of favourable environmental conditions, based on

13. IEA, 'Renewable Electricity', <https://www.iea.org/reports/renewable-energy-market-update-2021/renewable-electricity>, accessed 21 August 2021.
14. IEA, 'Renewables', <https://www.iea.org/reports/global-energy-review-2021/renewables>, accessed 21 August 2021; IEA, 'Renewables 2021: Analysis and Forecast to 2026', <https://iea.blob.core.windows.net/assets/5ae32253-7409-4f9a-a91d-1493ffb9777a/Renewables2021-Analysisandforecastto2026.pdf>, accessed 3 December 2021.
15. Liz Waters, 'Chapter 6: Renewable Sources of Energy', Department for Business, Energy & Industrial Strategy (BEIS), 2021, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1006819/DUKES_2021_Chapter_6_Renewable_sources_of_energy.pdf>, accessed 16 August 2021.
16. Ember, 'Global Electricity Review 2021: United Kingdom', 2021.

the global increase in renewables generation, their future remains on an upward trajectory.[17]

DEFINING 'RENEWABLES'

Renewables belong to a specific group of energy sources which are alternative to fossil fuels. Nuclear power is often spoken about publicly as synonymous with renewables such as solar or wind power. While nuclear energy sources are fossil fuel alternatives, they are non-renewable.[18] This research follows leading climate change and environmental organisations by adopting the International Renewable Energy Agency's definition of renewable electricity sources (see Table 1).

Table 1: Renewable Electricity Sources

Type	Definition
Wind	Wind turns the blades of a turbine around a rotor which spins a generator, turning the kinetic energy into electricity.[19] There are three main applications for wind turbines: • Onshore: a farm of wind turbines which are located on land. • Offshore: a farm of wind turbines which are located at sea or in fresh water. • Distributed: a small group of wind turbines that are installed closer to where the power is consumed, such as homes, schools and businesses.
Solar	There are two types of hardware involved in collecting solar power: • Photovoltaics (PV): cells within electronic devices (usually panels) which convert sunlight into electricity. • Concentrated solar power (CSP): mirrors are used to concentrate sunlight, which heats fluid and creates steam. The steam turns a turbine which generates electricity. This type of solar power is generated in large power plants.

17. BEIS, 'Energy Trends: UK, April to June 2021', statistical release, 30 September 2021, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/997347/Energy_Trends_June_2021.pdf>, accessed 29 November 2021.
18. This research is primarily concerned with renewable energy sources, which have minimal impact on the environment and ecosystems. Nuclear energy can have an adverse impact on the environment. For further details on nuclear waste and environmental impact, see US Energy Information Administration, 'Nuclear Explained: Nuclear Power and the Environment', <https://www.eia.gov/energyexplained/nuclear/nuclear-power-and-the-environment.php>, accessed 16 August 2021.
19. For further information on wind power, see International Renewable Energy Agency (IRENA), 'Wind Energy', <https://www.irena.org/wind>, accessed 29 November 2021.

Type	Definition
Ocean or tidal	Electricity can be generated through: • Tidal range technologies, such as a barrage, to capture the power generated between high tide and low tide. • Tidal current technologies, such as turbines. A hybrid application of the above.
Hydropower	Flowing water is used to spin a turbine which generates electricity.
Geothermal	Large amounts of steam produced by heat from under the Earth's surface are used for heating, cooling and to generate electricity.
Bioenergy	Energy is captured from the combustion of biomass such as wood and waste and is used to generate electricity.

Sources: For further information, see IRENA, 'Solar Energy', <https://www.irena.org/solar>, accessed 29 November 2021; IRENA, 'Ocean Energy', <https://www.irena.org/ocean>, accessed 29 November 2021; IRENA, 'Hydropower', <https://www.irena.org/hydropower>, accessed 29 November 2021; IRENA, 'Geothermal Energy', <https://www.irena.org/geothermal>, accessed 29 November 2021; IRENA, 'Bioenergy', <https://www.irena.org/bioenergy>, accessed 29 November 2021.

THE CURRENT STAKEHOLDER ECOSYSTEM AND POLICY LANDSCAPE

Stakeholder Ecosystem

With such a diverse stakeholder ecosystem, it is vital to clearly articulate which organisations are responsible for managing cyber risk in this sector. Key stakeholders include the UK government's Department for Business, Energy & Industrial Strategy (BEIS), which is responsible for enabling the overall shift to renewables and ensuring that energy is affordable and secure for UK consumers. The UK's independent regulatory authority for the energy sector, the Office of Gas and Electricity Markets (Ofgem) enforces statutory regulations on UK energy suppliers and ensures energy markets are operating fairly. The regulator also conducts various programmes to incentivise the shift to renewables and achieve net-zero targets, the most recent iterations being the Electricity Market Reform programme and the Contacts for Difference regime.[20] Both BEIS and Ofgem are responsible for overseeing the implementation of the 2018 Networks and Information Systems (NIS) Regulations in the electricity sector, which are discussed later in this section.

The National Cyber Security Centre (NCSC) is key to ensuring that energy providers make the shift to smarter, energy-efficient technology with security and resilience in mind. Through its Critical National Infrastructure (CNI) Hub, the NCSC supports energy providers by providing technical advice and best practices. It also provides guidance to Ofgem through its Cyber Assessment

20. Ofgem, 'Capacity Market and EMR Dispute Resolution', <https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/capacity-market-and-emr-dispute-resolution>, accessed 18 August 2021.

Framework (CAF) to help assess whether energy providers are appropriately managing their cyber risks.[21]

Since 1989, the UK's energy industry has predominantly resided within the private sector.[22] Companies are split based on their role in electricity transmission, distribution and supply.[23] There are four transmission operators who own and manage the electrical grid infrastructure:

- National Grid Electricity Transmission (England and Wales).
- Scottish Power Transmission.
- Scottish Hydro Electric Transmission.
- Northern Ireland Electricity.

As a separate entity, the National Grid Electricity System Operator (ESO) is responsible for transporting electricity across the UK and passing it on to Distribution Network Operators (DNOs). DNOs are companies who are licensed by Ofgem to distribute electricity from the national grid or transmission substations to homes, schools and businesses. There are 14 licensed DNOs owned by six different DNO groups.[24]

Companies that supply power to consumers buy the electricity from DNOs in the wholesale market. Traditionally, these UK markets have been dominated by six main companies: British Gas, EDF Energy, E.ON, Npower, Scottish Power and SSE. However, while the 'Big 6' have been diversifying their energy resources to include renewables, innovation and growth in the UK's renewable electricity industry stimulated by Ofgem regulations have paved the way for new entrants such as OVO Energy and Octopus Energy, which have seen a general increase in their share of the retail electricity market.[25]

21. National Cyber Security Centre (NCSC), 'NCSC CAF Guidance', <https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework>, accessed 18 August 2021.
22. Department of Energy & Climate Change, 'Energy Bill 2015–16, "Keeling" Schedule', January 2016, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/490992/Electricity_Act_1989__Energy_Bill_2015-16_Keeling_Schedule_.pdf>, accessed 29 November 2021.
23. Transmission networks carry electricity long distances around the country at high voltages; distribution networks run at lower voltages and take electricity from the transmission system into homes; and suppliers buy electricity from the wholesale or retail market and sell electricity to consumers.
24. For a list of all licensed Distribution Network Operator (DNO) groups and their respective DNO, see Nationwide Utilities, 'Distribution Network Operators (DNOs and IDNOs)', <https://www.nationwideutilities.com/service/dno-idno/>, accessed 29 November 2021.
25. Ofgem, 'Ofgem Breaks Down Barriers so Competition Can Work Better for Energy Consumers', 26 February 2014, <https://www.ofgem.gov.uk/publications/ofgem-breaks-down-barriers-so-competition-can-work-better-energy-consumers>, accessed 29 November 2021; Ofgem, 'Retail Market Indicators', <https://www.ofgem.gov.uk/energy-data-and-research/data-portal/retail-market-indicators>, accessed 29 November 2021.

Policy Landscape

The 2015 Paris Agreement is 'a legally binding international treaty on climate change'.[26] Its primary focus is for all 191 ratified states, including the UK, to commit to their own nationally determined contributions (NDCs) to limit global warming to 1.5 degrees and reduce CO2 emissions. Beyond the initial pledge, it emphasises the importance of technology through the implementation of a new technological framework.[27] This framework complements the Technology Mechanism that was established at COP16 in 2010 and aims to accelerate the global adoption of efficient and resilient climate technologies.[28]

UK-specific policy on the energy transition predates the Paris Agreement. The 2008 Climate Change Act created a system of carbon budgeting, which includes a cap on total emissions over a five-year period and outlined the UK's commitment to an 80% cut in the carbon emissions levels of 1990 by 2050.[29] In response to the Paris Agreement, this act was amended in 2019, with a new target of a 100% cut in emissions.[30] More recently, the UK government has made further commitments, such as expanding the use of low-cost renewables infrastructure and building digital infrastructure to aid the growing digitalisation of the energy sector.[31]

The 2018 Network and Information Systems (NIS) Regulations are vital to securing this digitalisation. NIS Regulations require all operators of essential services (OES), including energy, to effectively manage cyber risks to their respective sectors.[32] BEIS and Ofgem are the designated 'competent authorities' for the energy sector and are responsible for ensuring all OES are fulfilling the requirements highlighted in the NIS Regulations. There are also several standards that apply to the cyber risk management of

26. United Nations Framework Convention on Climate Change (UNFCCC), 'The Paris Agreement', <https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement>, accessed 29 November 2021.
27. UNFCCC, 'Technology Framework Under Article 10, Paragraph 4, of the Paris Agreement', <https://unfccc.int/sites/default/files/resource/cp24_auv_cop_4_TF.pdf>, accessed 29 November 2021.
28. UNFCCC, 'Technology Mechanism', <https://unfccc.int/ttclear/support/technology-mechanism.html>, accessed 29 November 2021.
29. It is important to note that CO2 emissions have supposedly fallen since 1990. For more details, see BEIS, 'Provisional UK Greenhouse Gas Emissions National Statistics 2020', 25 March 2021, <https://www.gov.uk/government/statistics/provisional-uk-greenhouse-gas-emissions-national-statistics-2020>, accessed 29 November 2021.
30. Legislation.gov.uk, 'The Climate Change Act 2008 (2050 Target Amendment) Order 2019: Explanatory Note', <https://www.legislation.gov.uk/uksi/2019/1056/note/made?view=plain>, accessed 29 November 2021.
31. HM Government, *Energy White Paper: Powering Our Net Zero Future*, CP 337 (London: The Stationery Office, December 2020).
32. Legislation.gov.uk, 'The Network and Information Systems Regulations 2018', <https://www.legislation.gov.uk/uksi/2018/506/made>, accessed 29 November 2021.

the energy sector. ISO/IEC 27001:2013 broadly outlines the requirements for 'establishing, implementing, maintaining and continually improving' information systems, and the key components for a cyber risk management framework.[33] ISO/IEC 27019:2017 applies the requirements outlined in ISO/IEC 27001:2013 to the process control systems used within the energy industry.[34] Additionally, the series of standards provided in IEC 62443 focuses on securing Industrial and Automation Control Systems and, due to increased automation of energy systems, is particularly important for ensuring the cyber resilience of the UK's evolving energy sector.[35]

At present, the NIS Regulations outline OES which are central to maintaining the security of the energy system within its existing structure. Yet, as the way energy is produced and distributed becomes more decentralised, the NIS Regulations will have to expand their reach to new types of operators who become integrated into the system. In this regard, one workshop attendee highlighted that although the NIS Regulations provide comprehensive and practical guidance on cyber risk mitigation to current energy industry operators, there is still work to do to ensure they can be effectively applied to new types of energy companies, such as electricity aggregators.[36]

TECHNOLOGY AND INFRASTRUCTURE

There are three layers of technology involved in energy infrastructure, including renewables, and they are defined in accordance with the National Institute of Standards and Technology (NIST) definitions:

- **Software**: 'Computer programs and associated data that may be dynamically written or modified during execution'.[37]
- **Hardware**: 'The physical components of an information system'.[38]
- **Firmware**: 'Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only

33. ISO, 'ISO/IEC 27001:2013', <https://www.iso.org/standard/54534.html>, accessed 29 November 2021.
34. ISO, 'ISO/IEC 27019:2017', <https://www.iso.org/standard/68091.html>, accessed 29 November 2021.
35. International Electrotechnical Commision, 'IEC 62443', <https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/>, accessed 6 December 2021.
36. An electricity aggregator is a new type of energy service provider which observes and moderates the electricity consumption of a group of consumers according to the overall demand of electricity on the grid. They also help sell excess electricity produced by a group of consumers back to the grid.
37. NIST, 'Software', <https://csrc.nist.gov/glossary/term/software>, accessed 29 November 2021.
38. NIST, 'Hardware', <https://csrc.nist.gov/glossary/term/hardware>, accessed 29 November 2021.

memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs'.[39]

Additionally, all major infrastructure is split between IT and OT layers. They are defined as:

- **IT**: 'Allows for the creation, storage, and exchange of information, usually via physical devices such as valves, computers, and storage, as well as software and networking equipment'.[40]
- **OT**: 'A system (hardware, firmware, and software) that detects and/or causes change through direct monitoring or control of physical devices, processes, and events in the system'.[41]

These elements of technology are then organised into the core and periphery infrastructure. This model is particularly important because of the decentralisation of energy generation (for example, a solar panel on a residential property or an electric vehicle charging point is part of the periphery infrastructure of the electricity sector).[42] The IoT is a vital element of the periphery in renewables due to their relative insecurity, which is explored in Risk 6. The core infrastructure is made up of centralised systems such as the electricity grid, where much of the control functionality lies in the ability to manage vast networks of electric vehicle chargers. This has an impact on cyber risk, which this paper articulates through the six risks it identifies.

DIGITALISATION OF ENERGY: THREE KEY CHANGES

Renewable electricity is a major area of investment, with technologists attempting to understand how to automate elements of energy production and improve efficiency.[43] As the industry continues to digitalise, understanding shifts in technology will help identify cyber risks. In this regard, there are three key changes related to the digitalisation of the energy sector: the convergence of IT and OT; the decentralisation and democratisation of energy production; and cloud convergence.

39. NIST, 'Firmware', <https://csrc.nist.gov/glossary/term/firmware>, accessed 29 November 2021.
40. Public–Private Analytic Exchange Program (AEP), 'Supply Chain Risks of SCADA/ Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions', 2017, <https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf>, accessed 29 November 2021.
41. Public–Private AEP, 'Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector'.
42. Consultative workshop, 10 March 2021.
43. *Bloomberg*, 'UK Renewable Power Set for a $27 Billion Investment Boost', 24 November 2020.

The Convergence of IT and OT

The convergence of IT and OT has been a game changer for energy production, distribution and supply.[44] Convergence is being driven by the benefits gained from increased automation of assets and operations, connected devices and sensors, predictive analytics, remote asset management, and flexibility to respond to ever-changing regulations as the sector innovates.[45] Underpinning the convergence of IT and OT is the increased use of SCADA in ICS.[46] SCADA systems have multiple uses, including monitoring and reporting data on a specific component of hardware, and offer the opportunity to automate controls and responses. As the industry digitalises, SCADA use will increase to manage a more dynamic energy environment.[47] An example of SCADA in renewables is consistent energy supply due to weather patterns, making it important to monitor the amount of energy that is being generated. SCADA components help to monitor renewable electricity infrastructure and further help to save energy when there are gaps in the supply.[48]

The Decentralisation and Democratisation of Energy Production

The second large shift in the energy sector is the decentralised model of production due to renewables. Where traditional electricity production was confined to power stations and industrial sites, renewable electricity provides a democratised model. The opportunity to install PV solar panels on the roof of a house at an affordable price point has helped to revolutionise how people produce energy. A decentralised energy system will not only reduce prices for homes, but potentially reduce national cyber risk as dependency on the grid is reduced in tandem.[49] The fewer homes that are dependent on the grid means fewer homes that may fall victim to a power outage if the grid is attacked.

The rise in renewables also has a knock-on effect for policymakers and countries that are traditionally exporters or importers of gas and oil due to limited infrastructure. Indeed, Indra Overland states that the trade relationship between producer and consumer countries will become more

44. Steve Livingston et al., 'Managing Cyber Risk in the Electric Power Sector: Emerging Threats to Supply Chain and Industrial Control Systems', Deloitte Insights, 2018; Public–Private AEP, 'Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector'.
45. Accenture, 'Building Greater Cyber Resilience in Renewables', May 2020.
46. See NIST, 'Supervisory Control and Data Acquisition (SCADA), <https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition>, accessed 29 November 2021.
47. Public–Private AEP, 'Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector'.
48. K Sayed and H A Gabbar, 'Chapter 18 – SCADA and Smart Energy Grid Control Automation', in Hossam A Gabbar (ed.), *Smart Energy Grid Engineering* (Cambridge, MA: Academic Press, 2016), pp. 481–514.
49. Hywel Lloyd (ed.), 'A Distributed Energy Future for the UK: An Essay Collection', Institute for Public Policy Research, September 2018.

symmetrical. Countries will be increasingly dependent on each other for renewables-based energy supplies, preventing monopolisation.[50]

Cloud Convergence

Cloud convergence has more complicated implications for digitalisation. Underpinning the increased digitalisation of the energy system and integration of IT and OT is its convergence with cloud-based infrastructure. The transition to cloud computing is seen as an essential part of utilising data from internet-connected devices.[51] By using cloud storage applications, energy service providers can store and remotely access the huge volume of data collected by SCADA from anywhere via the internet.

CYBER THREATS TO THE ELECTRICITY SECTOR

A variety of threat actors have demonstrated the intent and capability to target the electricity sector.[52] Although most existing cyber operations have not explicitly targeted renewables-based electricity production, transmission or distribution, this will likely change as the sector shifts to a reliance on renewables.[53]

The electricity sector is an attractive target for hostile state actors given its importance to national and economic security. In the UK, public reporting on operations by adversaries demonstrates that they have engaged in cyber espionage rather than sabotage or disruption. These types of operations are likely motivated by one of two objectives. First, growing demand for energy resources and technology means governments need to seek intelligence that would afford them a competitive advantage when vying for energy security.[54] Chinese threat actors, for instance, have been linked to a number of cyber espionage operations targeting North American and European organisations in the sector.[55] Given China's Made in China

50. Indra Overland, 'The Geopolitics of Renewable Energy: Debunking Four Emerging Myths', *Energy Research & Social Science* (Vol. 49, March 2019), pp. 36–40.
51. Abdur Rahim Biswas and Raffaele Giaffreda, 'IoT and Cloud Convergence: Opportunities and Challenges', *2014 IEEE World Forum on Internet of Things* (2014), pp. 375–76.
52. A 'threat' is normally defined as the intent and capability of adversaries to target an asset.
53. 'Likely' is defined against the intelligence community's probability yardstick, and suggests a 50–75% chance of something happening. See National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime', 2018.
54. FireEye, 'Cyber Threats to the Energy Industry', 2016, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-energy.pdf>, accessed 6 October 2021.
55. Christopher Glyer et al., 'This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits', Mandiant, 25 March 2020, <https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-

2025 industrial strategy identifies acquiring green technologies as a key objective, Chinese threat actors may be seeking commercial and technical intellectual property related to renewables. The second primary objective of state cyber espionage operations against the sector is reconnaissance of relevant ICS and SCADA to gather intelligence to enable future sabotage or disruption of electricity production or supply in the event of a conflict.[56] This is necessary because disruptive attacks against electrical utilities have, at least historically, required specialised malware and deep knowledge of targets' operational environments.[57]

There have also been at least two disruptive cyber attacks against the sector, albeit not in the UK. Most notably, threat actors linked to Russian intelligence carried out two separate attacks against Ukraine's electricity networks in the winters of 2015 and 2016.[58] These attacks formed part of a broader campaign against a range of CNI operators in Ukraine.[59] However, there is some scepticism about the likelihood of these types of operations being replicated outside of the Ukrainian context. Overland argues that the commonly cited Ukrainian power grid attack was a 'special case' created by a perfect storm of issues including 'dilapidated infrastructure, a high level of corruption, military conflict with Russia, and exceptional possibilities for Russian infiltration due to the historical linkages between the two countries'.[60] Moreover, there are deterrence considerations – namely, the threat of retaliation – that create restraints against disruptive operations against power networks in the US or its allies.[61] During the US–Russia summit in June 2021, for instance, President Joe Biden emphasised the possibility of cyber attacks against CNI being met in kind or with a conventional response.[62]

The electricity sector is an attractive target for hostile state actors

exploits>, accessed 6 October 2021; Michael Raggi and the Proofpoint Threat Insight Team, 'LookBack Forges Ahead: Continued Targeting of the United States' Utilities Sector Reveals Adversary TTPs', Proofpoint, 23 September 2019, <https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals>, accessed 6 October 2021.

56. See, for instance, Threat Hunter Team, 'Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group', Symantec, 20 October 2017, <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>, accessed 7 October 2021.
57. Dragos, 'Global Electric Cyber Threat Perspective', September 2021, <https://hub.dragos.com/hubfs/Reports/Global%20Electric%20Cyber%20Threat%20Perspective%20-%20Dragos%202021.pdf?hsLang=en>, accessed 6 October 2021.
58. *BBC News*, 'Ukraine Power Cut "Was Cyber-Attack"', 11 January 2017.
59. Booz Allen Hamilton, 'When the Lights Went Out: A Comprehensive Review of the 2015 Attacks on Ukrainian Critical National Infrastructure', <https://www.boozallen.com/s/insight/thought-leadership/lessons-from-ukranians-energy-grid-cyber-attack.html>, accessed 15 October 2021.
60. Overland, 'The Geopolitics of Renewable Energy'.
61. Anu Narayanan et al., *Deterring Attacks Against the Power Grid: Two Approaches for the U.S. Department of Defense* (Santa Monica, CA: RAND Corporation, 2020).
62. Vladimir Soldatkin and Steve Holland, 'Far Apart at First Summit, Biden and Putin Agree to Steps on Cybersecurity, Arms Control', *Reuters*, 17 June 2021.

At the same time, there are good reasons not to downplay the implications and consequences of the attacks against Ukraine's electricity sector. While the 2015 attack only affected 0.015% of Ukraine's daily electricity consumption and lasted just 1–6 hours,[63] disruption to the proper functioning of the affected power distribution companies lasted for several months.[64] Moreover, research by Dragos suggests that the 2016 attack could have been considerably more harmful. Analysis of the malware used in the operation indicates it was likely intended to cause physical damage to ICS in the affected power transmission station.[65]

While traditionally a key target for adversarial state actors, entities in the electricity sector have also recently attracted interest from ransomware groups involved in 'big game hunting', the practice where cybercriminals pursue higher potential returns by tailoring their operations to large enterprises operating critical assets. Although most ransomware strains are focused on IT rather than OT, they can still affect operations by impacting essential IT services. One notable example is the 2019 ransomware attack on Norsk Hydro, a Norwegian aluminium and hydroelectric power producer. The attack forced the company to shut down several plants and cost an estimated $71 million in downtime and recovery.[66] However, ransomware operators are now also directly targeting OT environments, and some ransomware strains – such as EKANS and Cl0P – include the ability to 'kill' ICS processes.[67] This raises the prospect of ransomware operations against electrical utilities causing considerable downtime.

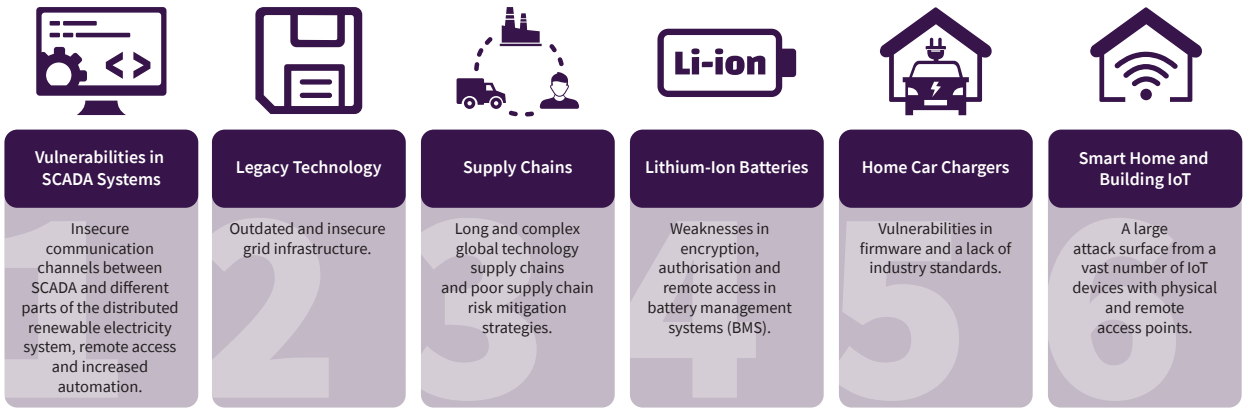
Finally, there is the potential for state adversaries to use ransomware for geopolitical purposes. Because ransomware is primarily associated with cybercriminals, it may provide cover for state threat actors. In May 2020, for instance, the Taiwanese government attributed ransomware attacks targeting the country's energy sector to a threat actor associated with the Chinese intelligence services.[68]

63. *Ibid.*
64. US Cybersecurity & Infrastructure Security Agency, 'ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure', updated 20 July 2021, <https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01>, accessed 15 October 2021.
65. Andy Greenberg, 'New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction', *Wired*, 12 September 2019.
66. Bill Briggs, 'Hackers Hit Norsk Hydro With Ransomware. The Company Responded With Transparency', Microsoft, 16 December 2019, <https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>, accessed 15 October 2021.
67. Dragos, 'Global Electric Cyber Threat Perspective'.
68. *Ibid.*

CYBER RISKS TO RENEWABLE ELECTRICITY PRODUCTION, DISTRIBUTION, STORAGE AND MANAGEMENT

While the three key changes highlighted in the previous section represent opportunities for innovation, they could also provide possible vulnerabilities. Furthermore, the aforementioned threats demonstrate the intent and capability to target future electricity infrastructure. With this in mind, this section outlines six cyber risks to renewable electricity production, distribution, storage, and consumer and business energy management technology. It consolidates the insights from existing technical literature into an accessible format.

Figure 1: Six Cyber Risks to Renewable Electricity Production, Distribution, Storage, and Consumer and Business Energy Management Technology



Source: Author generated.

To identify the six risks, the authors focused their research on the key areas of technology involved in the digitalisation of the energy sector as a whole, including renewables. For instance, to understand the cyber risks to renewable electricity storage, the authors used research into the cyber risks to lithium-ion batteries. This means that the risks identified here could equally apply to other areas where these technologies are being used and are only contextualised by their use in renewable electricity infrastructure.

PRODUCTION AND DISTRIBUTION

Managing the cyber risk of production and distribution requires an understanding of some of the key vulnerabilities in the value chain and whether they warrant risk mitigation. A study by Dragos found that 64% of industrial vulnerabilities do not introduce risk and a further 34% were inaccurate, leaving a mere 2% vulnerable. This challenges the commonplace 'patch at all costs' mindset of cyber risk management. Yet, no system is completely secure and understanding the 2% of industrial vulnerabilities can prevent major attacks.[69]

Risk 1: Vulnerabilities in SCADA Systems

As highlighted in the previous section, the increased importance of internet-connected SCADA systems in the production, distribution and overall management of renewable electricity systems

69. Dragos, 'Bridging the IT and OT Cybersecurity Divide', 2020, p. 10.

makes them an obvious target.[70] If an attacker gains access to SCADA system controls, the consequences could range from the loss of vital data and substantial financial cost to environmental damage.[71]

The key risk to SCADA stems from the growing number of connections it has to different devices and equipment across the energy system. In this regard, a significant area of compromise could be the communication channels between which different devices interact.[72] For instance, as SCADA analyses data collected in Wi-Fi-enabled devices, such as smart energy meters, vulnerabilities in these devices could act as backdoors, allowing for unauthorised access to any operation that SCADA manages.[73]

Similarly, vulnerabilities in remote access to SCADA systems could also be an issue. While many have emphasised the utility of virtual private networks (VPNs) for secure remote access, research has found critical vulnerabilities in industrial VPN servers which could give an attacker full access to remote systems.[74] Furthermore, the increased need for remote access, coupled with large amounts of data generated by SCADA, is encouraging operators to use cloud-based applications such as Platform as a Service (PaaS) and Software as a Service (SaaS). If improperly secured, the integrity of the data used by SCADA could be impacted, affecting the system's ability to make decisions.[75]

Increased automation of the system through SCADA has also been highlighted as a potential cyber risk. According to one workshop participant, the wide range of different devices connected through SCADA accompanying the shift to renewables will be more volatile and harder to control. This will require 'a much wider array of automated signals going across the grid which are potentially vulnerable to cyber attacks'.[76] The shift to predominantly digital

70. Erdal Irmak and Ismail Erkek, 'An Overview of Cyber-Attack Vectors on SCADA Systems', *2018 6th International Symposium on Digital Forensic and Security* (2018), pp. 1–5.
71. Jeffrey L Hieb, 'Cyber Security Risk Assessment for SCADA and DCS Networks', *ISA Transactions* (Vol. 46, 2007), pp. 583–94.
72. Alexander Bolshev and Ivan Yushkevich, 'SCADA and Mobile Security in the IoT Era', IOActive, 11 January 2018.
73. Public–Private AEP, 'Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector'; Sajid Nazir, Shushma Patel and Dilip Patel, 'Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques', *Computers & Security* (Vol. 70, September 2017), pp. 436–54.
74. Claroty, 'Getting From 5 to 0: VPN Security Flaws Pose Cyber Risk to Organizations With Remote OT Personnel', 28 July 2020, <https://www.claroty.com/2020/07/28/vpn-security-flaws/>, accessed 29 November 2021.
75. Rajesh Kalluri et al., 'Analysis of Communication Channel Attacks on Control Systems—SCADA in Power Sector', in Reji Kumar Pillai et al. (eds), *ISGW 2017: Compendium of Technical Papers* (2018), pp. 115–31; Mirjana D Stojanović, Slavica V Boštjančič Rakas and Jasna D Marković-Petrović, 'SCADA Systems in the Cloud and Fog Environments: Migration Scenarios and Security Issues', *Electronics and Energetics* (Vol. 32, No. 3, September 2019), pp. 345–58.
76. Consultative workshop, 10 March 2021.

substations associated with greater automation will mean that trips and safety protocols, which can be used to cut consumers' power, will become more networked and therefore more accessible to attackers.

Risk 2: Legacy Technology

A major cyber risk to energy distribution is legacy technology, as renewable electricity production is relatively new and distribution relies on older infrastructure, such as the national grid. One workshop participant further highlighted that the current focus on cyber security is more recent than the insecure protocols that were built and developed much earlier.[77] In addition, grid owners and operators are not incentivised to evolve newer technology because the old technology still functions, emulating an 'if it isn't broken, don't fix it' mindset. Incentives from a cost perspective to implement newer, more secure technology are missing.

However, the reality of investing in patching or replacing legacy technology was framed by one workshop participant as a juggle between driving investment and controlling the bills of their customers.[78] The way in which customers are priced for their energy is subject to a high level of public scrutiny because it contributes to living costs and is a necessity to the functioning of society. Companies simply cannot spend their way out of cyber risk. Moreover, considering the rapid onset of cloud convergence in energy systems, Dragos warns that connections between insecure legacy OT systems and cloud services could provide access to malicious cyber actors.[79]

Risk 3: Supply Chains

As emphasised by several workshop participants, an overarching cyber risk to the entire renewable electricity system stems from insecure technology supply chains.[80] If one vendor within the supply chain is compromised, this can have widespread consequences for all connected organisations. Recent high-profile examples of supply chain compromises include the SolarWinds and Kaseya attacks.[81]

Supply chains are a familiar issue in cyber risk management, involving a clear understanding of every stakeholder and third party in the value chain. Yet, as components are sourced from multiple countries, these supply chains are long and complex, making it difficult for companies to accurately map all vendors and subcontractors who supply each component. Additionally, as

77. *Ibid.*
78. *Ibid.*
79. Dragos, 'Bridging the IT and OT Cybersecurity Divide'.
80. Consultative workshop, 10 March 2021.
81. Kari Paul, 'What You Need to Know About the Biggest Hack of the US Government in Years', *The Guardian*, 15 December 2020; Jamie MacColl, 'The UK's Approach to Russian Cyber Operations Shows No Signs of Changing', *RUSI Commentary*, 14 June 2021; Brian Barrett, 'A New Kind of Ransomware Tsunami Hits Hundreds of Companies', *Wired*, 2 July 2021.

highlighted by one workshop attendee, these supply chains extend beyond the energy sector and cross other critical sectors such as telecommunications, maritime, healthcare and sewage facilities, which 'heightens the challenge of maintaining cyber resilience for all organizations in the supply chain'.[82]

The inability to effectively monitor supply chain risks is an ongoing challenge that both new and existing electricity suppliers need to address. A Deloitte report on the electricity sector states that 'most CISOs have no control over the enterprise's supply chain, and many have little access to supply chain cyber risk intelligence'.[83] Without knowing which of their suppliers are failing to prioritise cyber security, either because they are not properly resourced or because they are unwilling to invest, electricity suppliers cannot identify and mitigate any supply chain risk or enforce any liability if a vulnerability in their system is exploited.

As companies are shifting to digital infrastructure for data storage, one workshop attendee highlighted the added supply chain risk from cloud service providers (CSPs). At present, CSPs operate under a shared security model, meaning that the service user is responsible for securing the data that is being transmitted, stored and accessed and the cloud service provider is responsible for securing the infrastructure.[84] This increases the complexity of the supply chain as companies within the electricity system who use cloud services will have to account for risks coming from CSP supply chains. Furthermore, this is also complicated by the lack of transparency from CSPs around their risk mitigation strategies and the fact that cloud risk assessment is relatively underdeveloped.[85]

Equally, as supply chains are globalised, the UK is contending with the consequences of other states owning or playing a controlling role in their renewable electricity generators.[86] This presents its own cyber-related risks (for instance, the supply of poor-quality components could create vulnerabilities in hardware and software). Beyond the risk that cybercriminals could exploit these vulnerabilities, this introduces the possibility that malicious state actors may deliberately manipulate these technologies, so that they can be used to covertly collect data or enable

82. Marsh McLennan and Microsoft, 'Winning the Cyber Risk Challenge: Rapid Digitalization in the Energy/Power Sector Continues to Outpace Cyber Readiness', 2020.
83. Livingston et al., 'Managing Cyber Risk in the Electric Power Sector'.
84. Consultative workshop, 10 March 2021.
85. Olusola Akinrolabu, Steve New and Andrew Martin, 'Cyber Supply Chain Risks in Cloud Computing – Bridging the Risk Assessment Gap', *Open Journal of Cloud Computing* (Vol. 5, No. 1, 2018).
86. Michael Slezak, 'China Cementing Global Dominance of Renewable Energy and Technology', *The Guardian*, 6 January 2017; BEIS and Alok Sharma, 'New Powers to Protect UK from Malicious Investment and Strengthen Economic Resilience', 11 November 2020, <https://www.gov.uk/government/news/new-powers-to-protect-uk-from-malicious-investment-and-strengthen-economic-resilience>, accessed 6 December 2021.

a disruptive cyber attack on the UK's electricity sector. Much like in other areas of critical importance, policymakers must work closely with renewable electricity suppliers to ensure that key technology components comply with cyber security standards. Where standards are absent, governments should consider pushing for global implementation.

Nevertheless, in the UK, incentives to make companies think more about their supply chain risk are under way.[87] As one UK government official highlighted in the workshop, work is being done to 'create a supply chain assurance tool to ensure, during procurement, that there are key requirements for suppliers implemented by operators'.[88] Additionally, because supply chain issues are ubiquitous in all critical sectors, it is important to acknowledge that there is a wealth of existing guidance that can be applied to supply chains for renewable electricity systems.[89]

STORAGE

A major element of ensuring continuous energy supply to consumers is to store surplus energy. Wind patterns, sunlight and several other weather-related variables affect the amount of energy that is collected throughout the year. For instance, in summer, solar panels in the UK will collect a surplus of energy compared to winter. Therefore, to ensure enough energy is supplied during winter, storage is essential. Electricity is most efficiently stored through lithium-ion batteries. These batteries are commonplace (most smartphones have one, and electric vehicles use them to store electricity). The prominence of the lithium-ion battery is rising, and it plays a vital part in ensuring the UK reaches a net-zero future. However, there are cyber risks that could impair the battery's functionality and reliability.[90]

Risk 4: Lithium-Ion Batteries

The lithium-ion battery is well known for its attributes, including 'high power and energy density, long service life, low self-discharge, and no memory effect'.[91] As such, it has become the bedrock powering many devices today.

87. BEIS, 'Contracts for Difference for Low Carbon Electricity Generation: Government Response to Consultation on Changes to Supply Chain Plans and the CfD Contract', May 2021.
88. Consultative workshop, 10 March 2021; Pinsent Masons, 'UK Government Confirms Changes to Supply Chain Plans for Renewable Energy Projects', 27 May 2021, <https://www.pinsentmasons.com/out-law/news/uk-government-confirms-changes-to-supply-chain-plans-for-renewable-energy-projects>, accessed 29 November 2021.
89. Consultative workshop, 10 March 2021.
90. Megan Culler and Hannah Burroughs, 'Cybersecurity Considerations for Grid-Connected Batteries With Hardware Demonstrations', *Energies* (Vol. 14, No. 11, 2021), p. 2.
91. Taesic Kim et al., 'An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology', *IEEE Journal of Emerging and Selected Topics in Power Electronics* (2020).

Lithium-ion batteries use a battery management system (BMS) to 'ensure safety, reliability, and optimal operation'.[92] This includes monitoring the charge and health of the battery and control protection circuits, charging circuits and connection to external circuits.[93] There are three layers in lithium-ion batteries:

1. Communication and supervisory layer (connectivity to a network).

2. Control layer (control of hardware such as protection circuits).

3. Hardware layer (including, but not limited to, sensors and the thermal system).

The BMS is a point of exposure and potential vulnerability. Weaknesses in encryption, authorisation, remote access and much more can pose as potential entry points into the control layer. Taesic Kim and colleagues highlight that the state of charge can be changed, which is a potential risk to safe use of batteries as they can be set to overcharge.[94] They highlight the role IoT devices can play in increasing vulnerabilities, with some connected to the cloud.[95] This summary of vulnerabilities in lithium-ion batteries is surface level, and more research should be conducted to understand and examine the potential risks and mitigation that can be implemented as the importance of these batteries continues to rise.

CONSUMER AND BUSINESS ENERGY MANAGEMENT TECHNOLOGY

Smart meters, electric car chargers, solar panels and other 'local' touchpoints are central components of future consumer electricity use. This section focuses on two cyber risks in consumer energy technology and management because of their increasing prominence in homes. Home car chargers are increasingly common as plug-in hybrid and electric vehicles are becoming more popular across the globe. In addition, smart home IoT includes devices such as smart meters, smart thermostats and bulbs. In businesses, the infrastructure is more complex, with large-scale IoT management including a series of sensors built to measure, for example, CO2, temperature, humidity and occupancy.[96]

Risk 5: Home Car Chargers

Home car chargers are a unique point of intrusion because they serve a very specific purpose. In 2021, two home car chargers by manufacturers Wallbox

92. *Ibid.*
93. *Ibid.*
94. *Ibid.*
95. *Ibid.*
96. The EIC offers an example of how IoT sensors work in building management, and explains the technology layers involved. See EIC, 'IoT Building Energy Management', <https://www.eic.co.uk/services/intelligent-buildings/iot-building-energy-management/>, accessed 29 November 2021.

and Project EV were found to have significant firmware vulnerabilities that would enable an attacker to disable the charger or use it conduct attacks on other servers or chargers, in a similar way to a botnet.[97] It was also possible to infiltrate the wider home network the charger was connected to if the router admin password had not been changed. While these vulnerabilities have been patched, they provide good examples of how this technology is lacking in industry standards.

It should be noted that home car chargers are just one environment of risk. For businesses that rely on hauling physical goods, ensuring haulage companies have secure chargers for their vehicles will be a part of their risk calculus. Standards ensuring cyber security is embedded in chargers should be a priority for policymakers.

Risk 6: Smart Home and Building IoT

IoT devices in the smart home and building environment are central to the transition away from fossil fuels and towards a renewable electricity sector, as they equip users with information that helps them make more conscious decisions about their energy usage.[98] Smart home and building IoT are made up of a complex web of sensors and data points that have central remote access points. In the home environment, IoT can help energy management through remote access via a smartphone. In large buildings such as offices, companies use third-party vendors to supply software and data analysis on the efficiency of buildings. These software providers use IoT devices embedded in buildings to gather data from multiple points of use (for example, a smart thermostat on each level of the building). There are multiple layers in smart home IoT technology, including device hardware (the thermostat), a control hub and cloud connectivity.[99] There are multiple points of vulnerability within these layers.

Cyber risks to IoT are articulated by Brittany D Davis, Janelle C Mason and Mohd Anwar in their 2020 smart home case study. They found that there are four main 'buckets' of cyber risk: physical; network; software; and encryption. Table 2 outlines the different vulnerabilities in each.

97. Dan Simmons, 'Home Car Charger Owners Urged to Install Updates', *BBC News*, 3 August 2021.
98. According to Brittany D Davis, Janelle C Mason and Mohd Anwar, 'a smart home is composed of IoT devices and appliances that operate in a home environment'. See Brittany D Davis, Janelle C Mason and Mohd Anwar, 'Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study', *IEEE Internet of Things Journal* (Vol. 7, No. 10, 2020), pp. 10102–10.
99. Davis, Mason and Anwar, 'Vulnerability Studies and Security Postures of IoT Devices'.

Table 2: Vulnerabilities in Smart Home IoT

Type of Risk	Vulnerabilities
Physical	'Node tampering, radio-frequency (RF) interference on RF identifiers (RFIDs), node jamming in wireless sensor networks, malicious node injection, physical damage, social engineering, sleep deprivation,* and malicious code injection'.
Network	'RFID spoofing/cloning/unauthorized access, sinkhole, man in the middle, Denial of Service (DoS), routing information, and sybil'.
Software	'Phishing, malicious scripts, Trojan horse, spyware, adware, and DoS that exploit buffer overflows, SQL injections, and other types of vulnerabilities'.
Encryption	'Because IoT devices have limited computing power to support strong cryptographic protocols, they are vulnerable to the side channel, cryptanalysis, and man-in-the-middle attacks'.

Source: Brittany D Davis, Janelle C Mason and Mohd Anwar, 'Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study', IEEE Internet of Things Journal *(Vol. 7, No. 10, 2020), pp. 10102–10.*

* *Here, sleep deprivation relates to the device constantly being on, therefore potentially damaging physical components inside the hardware due to wear and tear.*

While these are a wide range of threats, there are real examples of vulnerabilities leading to misuse. For example, the NCC Group found that '97% of all attacks against smart devices' are to install the Mirai botnet, which 'probes for insecure devices, such as routers, wireless cameras and connected printers coming online'.[100] The UK government is not idle to the threat. In their recent Smart Systems and Flexibility Plan, BEIS and Ofgem recognised the need to 'embed a culture of cyber security across the smart energy system', as well as the need to have strong data collection and data sharing frameworks to ensure digitalisation is undertaken securely and with consumer privacy and security in mind.[101] In the plan, there is also a commitment to develop a regulatory framework which covers third-party organisations which are not currently being regulated (such as load controllers) to ensure they are their fulfilling the same cyber security requirements as other organisations within the energy sector.[102]

100. Andrew Laughlin, 'How a Smart Home Could Be At Risk From Hackers', Which?, 2 July 2021, <https://www.which.co.uk/news/2021/07/how-the-smart-home-could-be-at-risk-from-hackers/>, accessed 29 November 2021. For more information on the Mirai botnet, see Josh Fruhlinger, 'The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet', CSO, 9 March 2018, <https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>, accessed 29 November 2021.
101. BEIS and Ofgem, 'Transitioning to a Net Zero Energy System: Smart Systems and Flexibility Plan 2021', July 2021, p. 77.
102. *Ibid.*

Programmes, such as Secure by Design, pushing for new ETSI standards enforcing basic security measures in IoT devices was a significant first step.[103] Furthermore, the UK government may introduce a new law in 2021 that ensures manufacturers provide more support for IoT.[104] Legislation to reduce risk in the IoT will ultimately enable users to fully realise the advantages of smart home and building IoT in reducing their carbon footprint and transitioning to renewables.

CONCLUSION

The cyber resilience of the UK's renewable electricity sector is of seminal importance to ensuring the reliability and safety of a net-zero future. As well as an overview of the broad ecosystem of energy suppliers, producers, distributors, technology layers, areas of digitalisation and key cyber threats to the sector, this paper identified six high-level cyber risks to the future renewable electricity infrastructure in the UK:

1. Vulnerabilities in SCADA systems.
2. Legacy technology.
3. Supply chains.
4. Lithium-ion batteries.
5. Home car chargers.
6. Smart home and building IoT.

While an exhaustive examination of these risks is beyond the scope of this paper, their identification serves to introduce the nature of risk that exists in the sector, particularly for policymakers and new entrants to the discourse. The following policy-related questions require further research:

- To what extent can policy enforce cyber security regulations and standards in such a wide ecosystem of technology?
- What are the roles and responsibilities for the private sector in both implementing appropriate standards and regulations, but also being incentivised to go beyond the baseline?
- How can energy providers sufficiently map their supply chain, and to what extent is it realistic to assume that energy providers can appropriately ensure the cyber security of third parties?

103. Department for Digital, Culture, Media & Sport, 'Secure By Design', <https://www.gov.uk/government/collections/secure-by-design>, accessed 29 November 2021.
104. Andrew Laughlin, 'Smart Products Must Come Clean on Security Under New Laws', Which?, 21 April 2021, <https://www.which.co.uk/news/2021/04/smart-products-must-come-clean-on-security-under-new-laws/>, accessed 29 November 2021; BEIS and Ofgem, 'Transitioning to a Net Zero Energy System'.

- Are current standards in the IoT sector sufficient? What practical guidance should either the government or the private sector give to users on managing their devices?

The authors welcome research, such as that conducted by the World Economic Forum and the World Energy Council,[105] on understanding cyber risks to the renewable electricity sector and introducing risk mitigation strategies. However, there must be more research focusing on the UK context and potential policy to ensure risk mitigation is a priority for the private sector across the value chain.

ABOUT THE AUTHORS

Sneha Dawda is a Research Fellow in RUSI's Cyber Security research programme. She specialises in national cyber security strategies, internet governance, critical national infrastructure vulnerabilities and cybercrime.

Chamin Herath is a Research Analyst in cyber threats and cyber security. His research interests include cyber risks to critical sectors, policymaking around emerging technologies, online harms and violent extremists' use of the internet.

Jamie MacColl is a Research Fellow in cyber threats and cyber security. His research interests include cyber security, the evolution of the cyber threat landscape, the role of emerging technologies in security and defence policy and the uses of history in policymaking.

105. World Economic Forum, 'Net-Zero Challenge: The Supply Chain Opportunity', Insight Report, January 2021, <http://www3.weforum.org/docs/WEF_Net_Zero_Challenge_The_Supply_Chain_Opportunity_2021.pdf>, accessed 29 November 2021; World Energy Council, 'Cyber Challenges to the Energy Transition', 2019, <https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC_MMC_2019.pdf>, accessed 29 November 2021.

About RUSI

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 191 years.

Published in 2022 by the Royal United Services Institute for Defence and Security Studies. RUSI is a registered charity (No. 210639).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)