TER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Avoiding the internet of insecure industrial things

Lachlan Urquhart *, *Derek McAuley*

Horizon Digital Economy Research Institute, University of Nottingham, Nottingham, United Kingdom

Keywords:
Industrial internet of things
Cybersecurity
Network and information security
Data protection
Smart grids
Industrial control systems
Autonomous vehicles

A B S T R A C T

Security incidents such as targeted distributed denial of service (DDoS) attacks on power grids and hacking of factory industrial control systems (ICS) are on the increase. This paper unpacks where emerging security risks lie for the industrial internet of things, drawing on both technical and regulatory perspectives. Legal changes are being ushered by the European Union (EU) Network and Information Security (NIS) Directive 2016 and the General Data Protection Regulation 2016 (GDPR) (both to be enforced from May 2018). We use the case study of the emergent smart energy supply chain to frame, scope out and consolidate the breadth of security concerns at play, and the regulatory responses. We argue the industrial IoT brings four security concerns to the fore, namely: appreciating the shift from offline to online infrastructure; managing temporal dimensions of security; addressing the implementation gap for best practice; and engaging with infrastructural complexity. Our goal is to surface risks and foster dialogue to avoid the emergence of an Internet of Insecure Industrial Things.

1. Introduction to the industrial IoT

The industrial internet of things (IIoT) is an emerging commercial trend that seeks to improve management of the creation, movement and consumption of goods and services. It is part of a wider shift towards cyber physical systems (CPS) which are ". . .integrations of computation with physical processes. . .embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. . .".[1] IIoT is distinct from the consumer led IoT trend where ambient sensing occurs by remotely controllable and constantly connected physical objects embedded in domestic settings. These devices with a digital presence and backend computational infrastructure (e.g. cloud, databases, servers), networking and an

* *Corresponding author.* Horizon Digital Economy Research Institute, University of Nottingham Innovation Park, Triumph Road, Nottingham, NG7 2TU, United Kingdom.
E-mail address: lachlan.urquhart@nottingham.ac.uk (L. Urquhart).

Abbreviations: APTs, advanced persistent threats; CPS, cyber physical systems; C&Cs, command and control servers; CMA, UK computer misuse act 1990; DDoS, distributed denial of service; GDPR, general data protection regulation 2016; GPS, global positioning system; ICS, industrial control systems; IoT, internet of things; IIoT, industrial internet of things; NIS, network and information security; RFID, radio frequency identification.

[1] Edward A Lee, "Cyber Physical Systems: Design Challenges," *Technical Report No. UCB/EECS-2008-8*, 2008, http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html.

https://doi.org/10.1016/j.clsr.2017.12.004

associated ecosystem of stakeholders[2]. The IIoT departs by applying these technologies to industrial contexts. Instead of convenience, comfort or entertainment, the goal is to increase connectivity and track activity across supply chains.

IIoT is set for significant growth, estimated by Accenture to add $14.2 trillion to the global economy by 2023.[3] Major industrial investment in manufacturing, energy and transportation[4] is in automation, data driven sensing and actuation.[5] In a review of the domain, Xu et al highlight the following key use cases:

- Healthcare services – tracking healthcare inventory, global access and sharing of health data, and personalisation of patient care.
- Food supply chains – monitoring production from farm to plate including provenance tracking through Radio Frequency ID (RFID), distributed infrastructure and networking.
- Mining – safety applications like early warning sensing for natural disasters, chemical and biological sensors for worker disease detection underground.
- Transport and logistics – tracking physical objects being transported from origin to destination.
- Firefighting – detecting possible fires and providing early warning.[6]

Given the ubiquity of possible IIoT contexts, the breadth of risks can be vast, especially when intersecting with consumer led IoT.[7] For IIoT in healthcare, hacking of insulin pumps or pacemakers is a noteworthy concern.[8] Similarly, in the food supply chain, use of agricultural drones to survey farmland raises concerns for drone hacking, especially for larger vehicles.[9]

More broadly though, the industrial threat landscape already involves a multitude of actors utilising different IT vulnerabilities to leverage a variety of attacks.[10] These include:

- State sponsored hackers attacking foreign infrastructure either in advanced persistent threats (APTs) to steal military secrets or intelligence, or in patriotic campaigns to spread propaganda and interfere with foreign elections.[11] APTs often use zero day vulnerabilities (unpatched security flaws) in software to compromise critical infrastructure and steal confidential information.[12] There can also be **commercial cyber-espionage and sabotage** to obtain commercial intelligence, gain competitive advantage over rival businesses, and cause down-time.[13]
- Organised criminal groups **hacking** into organisations to access compromising information (e.g. trade secrets, emerging intellectual property, and evidence of malpractice).[14] They may also use malware campaigns to infect laptops or smartphones with remote access tools to record victims on their webcams in precarious acts and extorting them to prevent release of the footage as part of ransomware campaigns.[15]
- Loosely united hacker collective groups, like Lulzsec or Anonymous, use hacking or DDoS attacks[16] for social justice and retaliation against organisations for perceived immoral acts.[17] They will target websites or critical infrastructure to create service disruption and downtime, with associated financial and reputational costs.[18]
- Individuals can also create disruption. **Insider threats** posed by disgruntled employees involve use of their internal system access and credentials, or 'social engineering' attacks, to get sensitive information that can be traded with the highest bidder. [19] **Solitary** hackers breaking into military or na-

[2] Lachlan Urquhart and Tom Rodden, "New Directions in Information Technology Law: Learning from Human–computer Interaction," *International Review of Law, Computers & Technology* 31, no. 2 (2017): 1–19. – their working definition is derived from surveying a range of IoT stakeholder definitions e.g. Internet Engineering Task Force; International Telecommunications Union; Cisco; Internet Society etc.

[3] Accenture Technology, "Driving Unconventional Growth through the Industrial Internet of Things," 2015, https://www.accenture.com/gb-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf.

[4] World Economic Forum / Accenture, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services" (Cologny, 2015), http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

[5] Li Da Xu et al., "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics* 10, no. 4 (2014), doi:10.1109/TII.2014.2300753.

[6] Ibid.

[7] Derek O'Halloran and Elena Kvochko, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services," *World Economic Forum*, no. January (2015): 40.

[8] Iain Thomson, "BBC's Micro:bit Turns out to Be an Excellent Drone Hijacking Tool • The Register," *The Register*, 2017, https://www.theregister.co.uk/2017/07/29/bbcs_microbit_drone_hijacking_tool/.

[9] Jim Finkle, "J & J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking," *Reuters*, 2016, http://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUKKCN12411L.Lily Hay Newman, 'Medical Devices Are the Next Security Nightmare', *Wired*, 2017, https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.

[10] ENISA, *Threat Landscape Report 2016* (ENISA, Heraklion, 2017), 67–72.

[11] Dmitri Alperovitch, "Revealed: Operation Shady RAT," *White Paper*, 2011, https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[12] Brendan Koerner, "Inside the OPM Hack, The Cyberattack That Shocked the US Government," *Wired*, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[13] Thomas Rid, *Cyber War Will Not Take Place* (Hurst & Company, 2013); German Steel Mill example, discussed in more detail below.

[14] Marisa Randazzo et al., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," *Software Engineering Institute*, June 1, 2005, http://repository.cmu.edu/sei/457.

[15] Rebecca S. Portnoff et al., "Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights," *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems* 1 (2015): 1649–58, doi:10.1145/2702123.2702164.

[16] Distributed Denial of Service.

[17] Pammy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (Back Bay Books 2013).

[18] Argyro P. Karanasiou, "The Changing Face of Protests in the Digital Age: On Occupying Cyberspace and Distributed-Denial-of-Services (DDoS) Attacks," *International Review of Law, Computers & Technology* 28, no. 1 (January 15, 2014): 98–113, doi:10.1080/13600869.2014.870638.

[19] UN Office on Drugs and Crime, "Comprehensive Study on Cybercrime" (New York, 2013), https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

tional security infrastructure from their bedroom seeking to prove existence of UFOs or similar sometimes grab headlines as possible threats but ultimately spend years fighting unbending extradition processes.[20]

The advent of IIoT means vulnerabilities are becoming harder to detect and secure as systems go online. Sadeghi et al argue IIoT security is challenging because security countermeasures will develop slowly (often only prompted in the wake of attacks), the breadth of attack surfaces are wide (e.g. hardware, software, communication protocols etc.) and scope for system failures causing harm to property or humans is significant.[21]

The wealth of stakeholders operating in this domain is another practical issue. Large legitimate and illegitimate cybersecurity economies encapsulate security vendors, consultants and IT firms trying to patch or address threats contrasted with threat agents finding, stockpiling and trading vulnerabilities.[22] This diversity of actors can create confusion. The label 'hacker' is a useful example. Simply put, hackers can sit on a spectrum from law abiding 'white hats' to criminal 'black hats', with 'grey hats' sitting between the two. However, as we see above, it can include organised crime groups, state supported bodies and lone hackers, to name a few.

Weber argues that the only constant in cybersecurity is change, but that it is regulated in a fragmented manner.[23] He argues multiple stakeholders, particularly industry (who are most familiar with issues) and a breadth of regulatory mechanisms are needed to regulate IIoT.[24] Top down state centric legal approaches alone will not suffice.[25] In the privacy domain, we have argued the important role of non-state actors' practices in regulation, and the use of design orientated approaches to tackle regulatory harms from IoT.[26] Despite these challenges, the tide remains against IoT specific legislation in both US and EU, primarily due to desire to give the nascent industry a chance to sort itself out[27] instead favouring industry self-regulation or use of existing law.[28]

In practice whilst we see multi-stakeholder governance against cybersecurity harms, from regional laws to industry standards and initiatives, criminalisation by individual states remains a key global response to consider.[29] Cybercrime ordinarily entails traditional crimes enabled by IT infrastructure, like tax evasion, to true cybercrimes that would not exist but for the Internet, like bitcoin fraud, and hybrids that sit in the middle. [30] Crimes against IIoT are emerging, as are effective governance strategies. However, with criminalisation the law enforcement agencies already suffer skillset or resource deficits. These are coupled with procedural challenges of cooperating across borders to address heterogeneous, transnational cybercrimes.[31] Changes within the new EU 'Police and Justice' Data Protection Directive 2016[32] provides a framework for law enforcement agencies to cooperate and share data for investigations across borders, which may assist. Furthermore, the Council of Europe Cybercrime Convention 2001, discussed below, also contains controversial procedural powers around international cooperation and mutual assistance by states investigating and gathering evidence on crimes.[33] However, difficulties attributing attacks means criminal law may not be the most appropriate forum to redress harm. DDoS attacks, for example, could be deemed acts of cyberwar or terrorism (especially when critical infrastructure is targeted), acts of civil disobedience or protest,[34] or acts of commercial sabotage and for extortion. Adding the fear, uncertainty and doubt[35]

[20] The Guardian, "Gary McKinnon Resource Page," *The Guardian*, 2017, https://www.theguardian.com/world/gary-mckinnon.

[21] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner, "Security and Privacy Challenges in Industrial Internet of Things," in *Proceedings of the 52nd Annual Design Automation Conference on – DAC '15* (New York, New York, USA: ACM Press, 2015), sec. 4, doi:10.1145/2744769.2747942.

[22] Leyla Bilge and Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," *Proceedings of the 2012 ACM Conference on Computer and Communications Security – CCS'12*, 2012, 833–44, doi:10.1145/2382196.2382284.

[23] Rolf H. Weber and Evelyne Studer, "Cybersecurity in the Internet of Things: Legal Aspects," *Computer Law and Security Review* 32, no. 5 (October 1, 2016): 715–28, doi:10.1016/j.clsr.2016.07.002. - p721 and p728.

[24] Shackleford, S (2013) "Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance" American University Law Review 62(5) p1285, who lists these as 'laws and norms; market based incentives; code; self-regulation; public-private partnerships and bilateral, regional and multilateral collaboration"

[25] Ibid., 729.

[26] Urquhart and Rodden, "New Directions in Information Technology Law: Learning from Human–computer Interaction."

[27] European Commission (2013) Report on the Public Consultation on IoT Governance – p3; Weber p727; US Federal Trade Commission (2015) "The Internet of Things: Privacy and Security in a Connected World" Staff Report p7.

[28] Alliance for Internet of Things Innovation WG04 (2016) "Report on Policy Issues" p34.

[29] Samantha A. Adams et al., "The Governance of Cybersecurity The Governance of Cybersecurity: A Comparative Quick Scan of Approaches in," *TILT Working Paper*, 2015, https://pure.uvt.nl/portal/files/8719741/TILT_Cybersecurity_Report_Final.pdf.

[30] David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity, 2007); Ross Anderson et al., "Measuring the Cost of Cybercrime: A Workshop," *Workshop on the Economics of Information Security (WEIS)*, 2012, 1–31, http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf.

[31] David Wall and Matthew Williams, *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*, ed. Routeledge, 2014.

[32] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[33] Art 23–25.

[34] Lilian Edwards, "Wikileaks, DDOS and UK Criminal Law: The Key Issues | Practical Law," *Practical Law Company*, 2010, https://content.next.westlaw.com/Document/If375d9dee81911e398db8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1.

[35] With cyberwar see Richard A. (Richard Alan) Clarke and Robert K. Knake, *Cyber War: The next Threat to National Security and What to Do about It* (Ecco, 2010).

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

around securing IoT to the mix, and establishing strategies that balance the benefits of IIoT with measured governance responses is tough.

In this paper, we will consider the emergent smart energy supply chain as example of IIoT. This helps us dig into legal and, critically, technical perspectives, to reflect on security challenges posed by this trend. In Section 2 we frame our analysis using the example of the smart energy supply chain, as domain where numerous new vulnerabilities may arise. We discuss relevant legal issues in these sections. In Section 3 we dig deeper into problematic elements of new laws, particularly the NIS Directive and GDPR, and in Section 4, we consider technical responses. In Section 5 we offer brief conclusions.

2. Industrial IoT: from exploration to consumption

The anticipated ubiquity of networked devices embedded in infrastructure is exemplified by two current examples: smart cities and industry 4.0. The smart city movement[36] envisages urban infrastructure being upgraded to enable services like intelligent mobility[37] (e.g. congestion management, smart traffic lights, connected and autonomous vehicles) or smarter crime prevention, detection and prosecution (e.g. smart CCTV).[38] The scalability of IoT deployed in the city can frustrate effective management of security (and privacy) risks, partly due to the complexity of managing volume of data[39] and risks manifesting across interdependent systems. As Edwards states, "smart cities are a security disaster waiting to happen".[40]

Another context causing major concern is smart manufacturing (coined as 'Industrie 4.0' in Germany or the 4th Industrial Revolution)[41]. It entails using IoT to integrate business, production and engineering processes, to enable a smarter, more flexible and responsive supply chain.[42] However, increased automation in the workplace has already been shown to pose physical risks to human co-workers when errors occur (e.g. being crushed or killed by machinery).[43] Concurrently, informational risks are prevalent, with Symantec stating manufacturing is a key target for spear phishing attacks to steal system credentials (i.e. through targeted email/communications scams), especially for industrial control systems.[44]

To establish a concrete domain to unpack possible risks and threats, we focus on a case study, the emergent smart energy supply chain. The new NIS Directive, enforced from May 2018, already poses challenges for the existing energy sector, like satisfying notification requirements for incidents and putting in place adequate technical and organisational compliance measures.[45] Increased networking through smart energy systems will exacerbate the risks of non-compliance, if not done with adequate foresight. Building on these concerns, we want to explore possible risks at different points in the supply chain, prioritising the following elements: drilling for raw materials on a smart oil platform; when transporting material from platform to land using automated ships; with energy generation, transmission and distribution on the smart grid; with smart consumption and management by householders. This grounds our analysis, but many of the themes discussed are translatable to other industrial IoT contexts.

2.1. *The digital oilfield – IoT on oil platforms*

Whilst data is often called the 'new oil'[46], the adoption of IoT technologies into the oil and gas industry, has been quite slow.[47] Deloitte and others cite opportunities in the emerging 'digital oilfield' like predictive maintenance driven by low cost sensors, cloud computing and big data analytics.[48] However, an awareness gap around new technologies and their applications in the industry by professionals is keeping progress slow.[49] Nevertheless, as the digital oilfield expands, forecasting risks will be necessary to ensure sustainable development in this domain (for information, safety and environmental harms).

Focusing on exploration, specifically oil platforms, we can see how IoT might be utilised in oversight of drilling operations. The goal might be sensing and analysing information about how an operation progresses to spot possible choke points (esp. those creating maintenance down time) or where com-

[36] see Rob Kitchin's The Programmable City for critical engagement with the concept – http://progcity.maynoothuniversity.ie/resources/publications/.

[37] Giuseppe Anastasi et al., "Urban and Social Sensing for Sustainable Mobility in Smart Cities," in *2013 Sustainable Internet and ICT for Sustainability (SustainIT)* (IEEE, 2013), 1–4, doi:10.1109/SustainIT.2013.6685198.

[38] See David Murakami Wood and Michael Carter, "Power Down," *Limn*, 2017, http://limn.it/power-down/?doing_wp_cron=1495448151.7596950531005859375000.

[39] Rolf H. Weber, "Internet of Things: Privacy Issues Revisited," *Computer Law & Security Review* 31, no. 5 (August 2015): 618–27, doi:10.1016/j.clsr.2015.07.002.

[40] L. Edwards, "Privacy, Security and Data Protection in Smart Cities:," *European Data Protection Law Review* 2, no. 1 (2016): 28–58, doi:10.21552/EDPL/2016/1/6.e.

[41] Die Bundesregierung, "The New High-Tech Strategy," 2014; In UK see – New Strategy for Industry 4.0 Leadership https://www.out-law.com/en/articles/2017/october/industry-presents-its-vision-for-the-uk-to-become-a-leader-in-industry-40-/.

[42] Shiyong Wang et al., "Implementing Smart Factory of Industrie 4.0: An Outlook," *International Journal of Distributed Sensor Networks* 12, no. 1 (January 18, 2016): 3159805, doi:10.1155/2016/3159805.

[43] Justin Huggler, "Robot Kills Man at Volkswagen Plant in Germany – Telegraph," *The Telegraph*, 2015, http://www.telegraph.co.uk/news/worldnews/europe/germany/11712513/Robot-kills-man-at-Volkswagen-plant-in-Germany.html.

[44] Symantec, "Smarter Security for Manufacturing in the Industry 4. 0 Era," 2016, https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf.s.

[45] Out-Law, "The Network and Information Security Directive – Implications for the Energy Sector," Out-Law.com, 2017, https://www.out-law.com/en/topics/tmt–sourcing/cybersecurity/the-network-and-information-security-directive–implications-for-the-energy-sector-/.

[46] The Economist, "The World's Most Valuable Resource Is No Longer Oil, but Data," *Economist*, 2017, https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.

[47] GE, Accenture, and Junewarren-Nickle's Energy Group, 'Opportunities and Challenges for Digital Oilfield Transformation', 2015.

[48] http://dupress.com/articles/digital-transformation-strategy-digitally-mature/.

[49] Ibid.

ponents are not performing optimally (we outline an example in more detail in Section 3). Machine learning algorithms to spot trends and patterns in IoT sensor data could be deployed (similar to the different setting of mining, with Rio Tinto's autonomous trucks).[50] However, the distributed, task orientated and thus heterogeneous nature of sensors means different types of data could be fed back with varying quality and at intermittent time intervals. If one firm has worked out how to cut time for a drilling operation, say, enabling them to have lower running costs and undercut their rivals at bidding stage, then this is clearly valuable to competitors. As there are many different stakeholders/competitors sharing both infrastructure (e.g. physical oil rig facilities) and components (e.g. drilling tools). This creates risks for how to maintain confidentiality in operational information that could be fed back from IoT enabled devices, guarding against advanced persistent threats (APTs) or insider threats.[51]

In response, from a practical, and security perspective, instead of aggregating IoT data into larger datasets for remote analysis, as is the current 'big data analytics' trend, the growth of industrial IoT could prompt new architectures of secure, local analysis. Not reporting raw data wholesale, but instead statistical findings, could help make IoT sensor data useful for decision making about progression and direction of operations.[52] It could also address legal compliance concerns raised by cloud based storage and appropriate safeguards being in place e.g. Privacy Shield if a US based firm, binding contract clauses, adequate third countries etc.[53] Relatedly, ensuring security mechanisms are usable for workers is important. If an IoT system is too complex to use, or the steps necessary to maintain its security have too much scope for error, then human frailties may lead to vulnerabilities. The translation from offline to online world requires traditional Computer Supported Collaborative Work (CSCW) and human factors perspectives to understand how best to design secure, usable IoT systems that workers have skills to use.[54] Furthermore, as Craggs and Rashid argues for going beyond usability towards 'security ergonomics by design' i.e. ensuring systems think about users as an integral part of the system, particularly their well-being.[55]

On the drilling platform, organisational measures to address temporal dimensions of security are important too. Ensuring secure processes are maintained over time with workers is one dimension, supported by management processes and even health and safety training. But with IoT sensors and components, there are additional risks. Securing the streams of data from IoT sensors and actuators requires maintained oversight of vulnerabilities and patching infrastructure when necessary, e.g. IoT device firmware. Preventing tampering in devices, and ensuring legacy information is not left behind moved between platforms, or even decommissioned may be necessary to ensure confidential information is not shared. Ongoing cyber-espionage activities/APTs are increasing, as high-profile campaigns like Operation Shady RAT or Operation Aurora show. These ordinarily involve targeting of state and large-scale industrial infrastructure to steal foreign intellectual property and intelligence, to assist the economic and strategic interests of the perpetrators.[56] The actors involved in these campaigns range from state sponsored hacking groups to nation states, making identification of sources, and thus appropriateness of response difficult to establish. Information from IoT on oil platforms could be another target for such campaigns, as we explore in Section 3.

2.1.1. *Insider attacks and unauthorised access*

Insider attacks could involve an employee accessing the rig IT system to load and execute malware or steal secrets for later sale. This could incur prosecution under unlawful access/'hacking' provisions in s1 Computer Misuse Act (CMA) 1990 (and s3 CMA for malware execution). The three part s1 CMA offence occurs when a person causes a computer to:

1) "perform any function with intent to secure access to any program or data held in any computer[57], [or to enable any such access to be secured]'";
2) where 'the access he intends to secure [or to enable to be secured] is unauthorised,' and
3) "he knows at the time when he causes the computer to perform the function that that is the case'".[58]

'Securing access' means the person causes the computer to perform any function results in alteration or erasure of data, copying or moving data, causes a program to run, and so forth.[59] 'Unauthorised access'[60] is when the person is not 'entitled to control access. . .' and lacks consent from the one who is

[50] Aimee Chanthadavong, "Rio Tinto Digs for Value in Data," *ZDNet*, 2015, http://www.zdnet.com/article/rio-tinto-digs-for-value-in-data/.

[51] Anshu Mittal Andrew Slaughter, Gregory Bean, 'The Internet of Things in the Oil and Gas Industry', *Deloitte Insights*, 2015, https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-oil-and-gas-industry.html (all URLS last accessed on 26 Sept 2017); GE, Accenture, and Junewarren-Nickle's Energy Group, 'Opportunities and Challenges for Digital Oilfield Transformation', 2015.

[52] Hamed Haddadi et al., "Personal Data: Thinking Inside the Box" (London/Cambridge, 2015), doi:10.7146/aahcc.v1i1.21312.

[53] Christopher J. Millard, *Cloud Computing Law* (Oxford: OUP, 2013), doi:10.1017/CBO9781107415324.004.

[54] Sara Kraemer, Pascale Carayon, and John Clem, "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities," *Computers and Security* 28, no. 7 (October 1, 2009): 509–20, doi:10.1016/j.cose.2009.04.006.

[55] Barnaby Craggs and Awais Rashid, "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design," in *Proceeding - 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems, SEsCPS 2017*, 2017, 22–25, doi:10.1109/SEsCPS.2017.5.

[56] Alperovitch, "Revealed: Operation Shady RAT"; Jim Finkle, "Hacker Group in China Linked to Big Cyber Attacks: Symantec," *Reuters*, September 17, 2013.

[57] s17(6) includes "references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium."

[58] CMA 1990 s1(1)(a) -(c) as Amended by Police and Justice Act 2006 c 48 Pt 5 s35 in brackets.

[59] s17(2) CMA 1990.

[60] s17(5) CMA 1990.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

entitled.[61] Case law helps us unpack s1 CMA further. Attorney General's Reference (No 1 of 1991) [1993] Q.B. 94 clarified it does not require use of a different computer for unauthorised access, but instead can be from the same computer.[62] In DPP v Bignall [63] authorised access to the Police National Computer was used to obtain private information. Despite the Department of Public Prosecutions (DPP) claiming this was 'unauthorised access', as their access was only meant to be for police purposes, the court found this was not a breach and "a person does not commit an offence under the 1990 Act, s1 if he accesses a computer at an authorised level for an unauthorised purpose".[64] A few years later this all changed in R v Bow Street Magistrates Court ex Parte Allison No 2[65] which held s1 CMA can cover activities of employees accessing data they were not authorised to.[66] The House of Lords defined scope of s1 CMA stating it "refers to the intent to secure unauthorised access to any programme or data. These plain words leave no room for any suggestion that the relevant person may say: 'Yes, I know that I was not authorised to access that data but I was authorised to access other data of the same kind.' ".[67] Insider attacks using existing login credentials would be covered by this provision, providing a route of recourse in the event of breaches.

2.2. *Autonomous systems in logistics – smart oil tankers*

Use of autonomous systems in logistics is a clear application area for the industrial IoT. The shift towards autonomous ships (AS) is a good example, as shipbuilders across the world are investing in revolutionising transport of cargo globally (e.g. Rolls Royce).[68] Like with autonomous cars, different stages of automation will exist, and interaction between autonomous and current ships will continue.[69] For oil industry, smart oil tankers or supply vessels would be a possible application domain. Naturally, such use of AS brings a new forum for security threats to manifest. Ransomware from hackers is a big one to consider. GPS jamming, spoofing or scrambling could be used to manipulate ships or threaten to run them aground, causing financial cost and significant environmental harm (especially if the cargo is oil) unless a ransom is paid to attackers.[70] Similarly, it could present a new forum for international piracy to play out, where theft of ships is done remotely, without pirates ever needing to even set sail. Depending on the level of autonomy a ship has, insider threats would be another concern, e.g. for sabotage. On a spectrum of full to partial, manned or unmanned, this could shape to what extent insider threats manifest on board, and strict controls on who has remote access to the ship need to be maintained.

These concerns align with a wider trend towards ransomware and extortion campaigns, which have increased hugely in recent years,[71] leading ENISA to estimate such activity has generated a global turnover of $1bn in 2016.[72] Malware was the dominant cybersecurity threat of 2016,[73] and it has become more targeted, as financial Trojans used in the 2016 Bangladesh Bank heist show (where $81m was stolen through fraudulent transactions).[74]

The vulnerabilities posed by a recent ransomware attack, 2017's WannaCry, highlight risks of longitudinal security management in industrial IoT futures. WannaCry spread in IT systems across the globe exploiting a vulnerability in legacy system, Windows XP, which was released in 2001. The malware encrypted files stored on a system, demanding payment to decrypt and regain access. WannaCry caused widespread disruption to critical infrastructural services, for example operations and appointments at hospitals. Whilst not targeted directly at specific organisations, many services are still using XP with the vulnerability unpatched, hence it has spread far, quickly. The UK National Health Service, Spanish telecoms giant Telefonica, US logistics firm FedEx and German rail network Deutsche Bahn were all victims. For some organisations, difficulties are compounded by challenges updating systems at scale in organisations, where funding for IT services is inadequate, e.g. public sector, healthcare etc. This may be less of a risk for oil and gas sector.

In the context of smart logistics in the oil industry, utilising AS, the desire for integration between operational and management IT could increase exposure to malware. Diminishing vendor support over time, as in the case of Microsoft, would be another concern. Given the poor IoT state of emerging se-

[61] Amended by Criminal Justice and Public Order Act 1994 c.33 Pt XII s.162(2) (1995) section 10 relates to use of other law enforcement powers.

[62] E.g. by "*using another person's identifier (ID) and /or password without proper authority in order to access data or a program; displaying data from a computer to a screen or printer; or even simply switching on a computer without proper authority*." J. Zoest 'Computer Misuse Offences' (2014) *Westlaw UK Latest Update* p1-.

[63] [1998] 1 Cr. App. R. 1.

[64] Halsbury's Laws of England, Supplement to 11(1) (4th Ed Reissue) para 604A.

[65] (AP) [2000] 2 AC 216.

[66] [1999] 3 W.L.R. 620.

[67] [2000] 2 A.C. 216 at 224.

[68] Rolls Royce, "Autonomous Ships: The Next Steps," *Rolls Royce*, 2016, http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/rr-ship-intel-aawa-8 pg.pdf.

[69] SAE international, "New SAE International Standard J3016," *SAE International*, 2016, doi:P141661.s.

[70] Matt Burgess, 'When a Tanker Vanishes, All the Evidence Points to Russia' *Wired UK*, 2017 <https://www.wired.co.uk/article/black-sea-ship-hacking-russia?utm_content=bufferc8256&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer> accessed 26 September 2017; Oeystein Glomsvoll and Lukasz K Bonenberg, 'GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea' (2017) 70 Journal of Navigation 33.

[71] National Cyber Security Centre and National Crime Agency, "The Cyber Threat to UK Business" (London, 2017), 5, http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file. show a growth in cyber extortion; Recent Bad Rabbit Malware as another example see – http://www.bbc.co.uk/news/technology-41740768.

[72] ENISA, "ENISA Threat Landscape Report 2016," 43.

[73] It is top threat in ENISA, "ENISA Threat Landscape Report 2016."; Rebecca Klahr et al., "Cyber Security Breaches Survey 2016" (London, 2016), 4, doi:10.13140/RG.2.1.4332.6324.p4 states "*the most common types of breaches experienced are viruses, spyware or malware (68%) and breaches involving impersonation of the organisation (32%)*"

[74] National Cyber Security Centre and National Crime Agency, "The Cyber Threat to UK Business," 7.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

curity practices, guarding against industrial IoT ransomware is a daunting prospect. Resources for patching vulnerabilities in a distributed network of devices, controlled by different stakeholders in a supply chain, would be logistically and practically complex. The interdependent nature of critical infrastructural systems, especially in a sector like oil with extensive outsourcing to service firms, would add another layer of difficulty. Whilst it is clear getting security right for the emerging industrial IoT is critical to ensure long term resilience and prevent substantial costs down the line, practically doing this is another matter.

2.2.1. *Resilience and criminalising material damage*

In ensuring IoT resilience, dual use tools, such as penetration test networks, have posed challenges for s3A UK CMA 1990 in the past.[75] s3A is designed to control trade in tools used for computer misuse offences by criminalising making, adaptation, supply or offer to supply articles suppliers believe it is likely to be for use/to assist in commission of CMA offences.[76] The Crown Prosecution Service has now clarified mere possession of such articles, is not an offence, without requisite intent.[77] Intent depends on factors like, normal use cases, if the article is commercially available (or only for offences) and who uses it. These wide parameters mean creating resilient IoT may still require reflection on tools used and their legal appropriateness.

Furthermore, if IIoT infrastructure is not resilient, and subject to attack, s3ZA CMA[78] criminalises causing serious damage. It applies when the accused does any unauthorised act in relation to a computer; knowing at that time it is unauthorised; causing, or creating a significant risk of serious damage of a material kind; and intending, by doing the act, to cause such damage or being reckless as to if it is caused.[79] Material damage could include to the environment or human welfare in any place or to the economy or national security of any country.[80] Material damage to human welfare is quite broad, ranging from loss of human life, illness, or injury; disruption to supply of money, food, water, energy or fuel; disruption of communications systems, transport facilities or health services.[81] When causing material damage, it is immaterial if the act causes the damage directly, or is the only or main cause of the damage.[82] Doing an act includes causing an act to be done, including if it is a series of acts. A country includes reference to a territory, and any place in, or part or region, of a country or territory.[83] This broad provision has scope for use against perpetrators of cyber-attacks that cause significant damage to critical infrastructure. In the context of IIoT, if a perpetrator can be established, attacks causing black-outs impacting emergency services or the stock exchange, damage to ICS/SCADA (particularly in nuclear power stations) or general downtime for smart infrastructure, would conceivably be covered.

2.3. *Smart grid and meters – generation, transmission/distribution and consumption*

2.3.1. *Generation*

In the context of energy generation, the IT systems used by factories and power plants are already at risk, providing a warning for what happens when infrastructure is networked. Most concern is around vulnerabilities in industrial control systems (ICS), which come in a number of varieties but largely "consists of a combination of control components (e.g. electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g. manufacturing, transportation of matter or energy)".[84] Traditionally, ICS are 'air-gapped' (i.e. not connected to the internet) to limit vulnerability to external attacks which can cause physical harm. This means, threats often emerge from actors physically booting vulnerabilities locally, e.g. via USB. But with the growth of the industrial IoT and networked integration across systems, this safeguard is being removed.[85] Traditional phishing campaigns are a risk,[86] and an attack on Ukrainian electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo led to blackouts and power outages and affected over 220,000 customers and utilised malware distributed through phishing emails and malicious Microsoft Word files.[87] Malware linked to these Ukrainian attacks, Industroyer, is particularly dangerous because it enables control of substation switches and circuit breakers.[88]

Exploitation of zero day vulnerabilities against ICS used in power plants and factories like SCADA,[89] a type of ICS defined by US Standards agency NIST as "systems [that] are used to control dispersed assets where centralized data acquisition is as important as control. . ." are also prevalent.[90] A recent SCADA

[75] As amended by the s41 Serious Crime Act 2015; See Edwards (2010) at section 'is merely downloading the LOIC a crime?'

[76] s3A (1–3) CMA – other offences of s1, s3 or s3ZA CMA 1990.

[77] Crown Prosecution Service Legal Advice on Computer Misuse Act 1990 available at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/.

[78] Added by s41 Serious Crime Act 2015.

[79] s3ZA (1).

[80] s3ZA (2).

[81] s3ZA (3) CMA 1990.

[82] s40(4).

[83] s40(5).

[84] Keith Stouffer et al., "Guide to Industrial Control Systems (ICS) Security," *NIST*, 2015, doi:10.6028/NIST.SP.800-82r2.2-1.

[85] ENISA, "Protecting Industrial Control Systems: Recommendations for Europe and Member States" (Heraklion, 2011); Barak Perelman, "Air Gap or Not, Why ICS/SCADA Networks Are at Risk | SecurityWeek.Com," *Security Week*, 2016, http://www.securityweek.com/air-gap-or-not-why-icsscada-networks-are-risk.

[86] ENISA Smart Grid Recommendations 2012.

[87] HM Government, "National Cyber Security Strategy 2016–2021," 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[88] John Leyden, "Move Over, Stuxnet: Industroyer Malware Linked to Kiev Blackouts • The Register," *The Register*, 2017, https://www.theregister.co.uk/2017/06/12/industroyer_malware/.

[89] Vinay M. Igure, Sean A. Laughter, and Ronald D. Williams, "Security Issues in SCADA Networks," *Computers and Security* 25, no. 7 (2006): 498–506, doi:10.1016/j.cose.2006.03.001.

[90] Stouffer et al., "Guide to Industrial Control Systems (ICS) Security." s2-5 continues "[examples] *distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems. . .SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time.*"

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

hack targeting a German steel mill suffered physical damage in 2015.[91] However, arguably the highest profile targeted ICS attack was the state sponsored 2010 Stuxnet worm attack (allegedly from the US and Israel)[92] on the Iranian Natanz nuclear enrichment plant. It targeted a specific Siemens ICS, using a combination of fake authentication certificates and zero day exploits[93] to reach its target and deploy a complex payload designed to vary speed at which uranium enrichment centrifuges spin, thus destroying them. The payload slowed production at the plant, as centrifuges had to be replaced more quickly. Ultimately, it aimed to delay production of purportedly nuclear weapons using enriched uranium as part of the Iranian Nuclear program.[94] For industrial IoT, these cases highlight the need for careful consideration about what should and should not be networked and connected to the Internet, relative to costs and benefits (both economic and security).

2.3.1.1. *Addressing ICS hacks*. Targeting critical civilian infrastructure, like ICS, as the 'battlefield' for playing out international tensions complicates navigation of this domain.[95] The international law on cyberwarfare may come to the fore, both with the jus ad bellum and jus in bello.[96] The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn has sought to create clarity, through the Tallinn Manuals. These interpret application of public international law to cyber operations during armed conflict[97] and more recently, during peacetime.[98] They focus on use of force and self-defence in Article 2(4) and Article 51 of the UN Charter, beyond the original scope of armed attacks causing kinetic damage. As mentioned before, attributing attacks is tricky, especially when it is the basis for justifying action between nation states. Network traffic can be masked and routed via several countries to hide the identity of perpetrators, making establishment of state responsibility for cyber-attacks difficult.[99] Furthermore, given the messy crossover between cyberwar, crime, espionage, and terrorism, to name a few, holding nation states responsible for acts of groups acting autonomously within their borders is tough. This is especially if such groups do so without knowledge or authority of the armed forces. Questions of proportionality of responses to interstate cyber-attacks also requires political and ethical reflection. Even if kinetic attacks in response to cyber-attacks can be deemed legal,[100] is it morally correct to do so? With states designing and building cyber weapons like Stuxnet, is a cyber arms trade treaty needed to control weapon use or even for a ban banning some, as with nuclear weapons or chemical weapons?[101] Nevertheless, despite all these difficult questions, some experts suggest the risks are overstated.[102] Instead, perhaps we need to refocus on the more mundane threats to power grids – electrocuted squirrels and birds causing outages.[103]

2.3.2. *Transmission*

Industry and government are driving the shift towards smart grids, i.e. "an upgraded energy network to which two-way digital communication between the supplier and consumer, smart metering and monitoring and control systems have been added".[104] The grid aims to create more efficient energy production by industry, smarter consumption by citizens and works towards domestic, regional and international CO2 emission reduction targets.[105] Levelling off inefficient peaks in consumer demand is a goal, relying on more than just understanding consumer behaviours, but changing them. Pricing is one mechanism, and consumers could be incentivised to change habits through time of use (TOU) tariffs i.e. where electricity pricing changes at different times of the day.[106] There are security risks here in malicious manipulation of supply and demand, for economic loss by both providers and consumers (especially with consumption being measured by smart meters, more on this below). Smart grid security has had strategic attention from bodies like ENISA, with numerous best practice documents requiring resilience by design technical means (e.g. end to end security)

[91] Kim Zetter, "Car Wash Hack Can Strike Vehicle, Trap Passengers, Douse Them With Water – Motherboard," *Motherboard*, 2017, https://motherboard.vice.com/en_us/article/bjxe33/car-wash-hack-can-smash-vehicle-trap-passengers-douse-them-with-water.z.

[92] Ellen Nakashima and Joby Warrick, "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say – The Washington Post," *The Washington Post*, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.9ee2a60c2170.

[93] I.e. unpatched vulnerabilities in IT systems that can be exploited. A market exists in buying these exploits before they are patched by vendors.

[94] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, 2011.

[95] For even more detail, the Special Edition on Cyberwarfare of Journal of Conflict and Security Law (2012) – Vol 17:2 - http://jcsl.oxfordjournals.org/content/17/2.toc.

[96] H H Dinniss, *Cyber Warfare and the Laws of War*, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), doi:10.1017/CBO9780511894527.

[97] Split into 2 parts – Part I International Cybersecurity Law (i.e. primarily the jus ad bellum) with state attribution (Rules 6–9); Use of Force (10–12); Self Defence (13–17); then Part II on Law of Cyber Armed Conflict (i.e. primarily the jus in bello) with detailed rules on cyber weapons, legitimate targets, cyber espionage and the nature of attacks (Rules 25–66).

[98] CCD COE NATO, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Tallinn: Cambridge University Press, 2017); CCD COE NATO, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn: Cambridge University Press, 2013).

[99] Jeffrey Carr, "Responsible Attribution: A Prerequisite for Accountability," *The Tallinn Papers: A NATO CCD COE Publication on Strategic Cyber Security*, 2014, https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn Paper No 6 Carr.pdf.

[100] David Alexander, "U.S. Reserves Right to Meet Cyber Attack with Force | Reuters," *Reuters*, 2011, http://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116.

[101] Arimatsu (2012) "A Treaty for Governing Cyber-Weapons" *CCD COE Cycon* http://www.ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf.

[102] Rid, *Cyber War Will Not Take Place*.

[103] Cleve Wootson Jr, "Most Cybersecurity Experts Are Worried about Russian Hackers. One Says: Look, a Squirrel!," *The Washington Post*, January 2016. http://www.cybersquirrel1.com/#;

[104] Communication 2012/148/EC Section 3(a) Definitions.

[105] The UK DECC need to reduce CO2 by 80% by 2050 from 1990 levels, in line with the UK Climate Change Act 2008 and Energy Act 2011.

[106] e.g. cooking between 5 and 8pm or having showers between 6-8am.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

and organisational ones (e.g. risk assessments).[107] A particular risk that is hard to manage is distributed denial of service (DDoS) attacks, often facilitated by botnets.

There is an extensive number of botnets and a 2013 UN Office on Drugs and Crime Comprehensive Study on Cybercrime estimated around 1 million botnet C&Cs globally, with high volume clusters in Eastern Europe, Central America, and the Caribbean.[108] Devices compromised by malware become infected "zombie" units, enslaved to a command and control server which remotely controls their behaviour on demand. Botnets are then put to work, often for hire, for DDoS campaigns, by a range of actors, from organised crime groups to script kiddies.[109] DDoS attacks flood servers with requests, meaning services hosted on targeted servers are knocked offline temporarily, but DDoS attacks are not permanent and impacts often resolved once servers are brought back online.[110] For the smart energy grid, DDoS attacks could impact transmission and distribution networks, leading to power outages and associated black outs, where physical safety is at stake.[111] Furthermore, it can impact flows of information between consumers and producers, where costs go beyond downtime but also disrupting production schedules, leading to significant economic, safety or political costs as second order effects are felt down the supply chain.

2.3.2.1. *Confronting DDoS.* Whilst Internet Service Providers have a role to play in monitoring and throttling high volumes of traffic, criminally tackling DDoS pushes us to s3 CMA 1990. It covers 'unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer. . .'. Such acts (or a series of acts) can involve temporary impairment, prevention or hindering operation of a computer, being indiscriminate towards computers, programmes or data. As DDoS attacks do not ordinarily cause permanent damage to the server, merely knocking it offline temporarily, they still come within the scope of s3. The DPP v Lennon (2006) examined[112] a mail bombing campaign committed by Lennon against a former employer's servers.[113] The court accepted sending emails was a modification to a computer (before 2006, s3 required unauthorised 'modification' instead of an 'act').[114] The case focused on the authority for this act, especially when sending emails is ordinarily an authorised activity. The court held that the implied consent of a user to receive emails is not without limits,[115] and such consent does not stretch to cover situations where the purpose of emails is to overwhelm the system, as is the case with DDoS too. Lord Justice Keene stated the recipient "does not consent to receiving emails sent in a quantity and at a speed which are likely to overwhelm the server. Such consent is not to be implied from the fact that the server has an open as opposed to a restricted configuration."[116] Accordingly, there is precedent around DDoS type attacks flooding a server with requests, and this would criminalise DDoS attacks against IIoT infrastructure e.g. targeting components of the supply chain.

2.3.3. *Consumption*

As part of the smart grid, homes around Europe (and the world) are being fitted with smart meters i.e. 'electronic systems that can measure energy, consumption, providing more information than a conventional meter, and can transmit and receive data using a form of electronic communication'.[117] In the UK, the Smart Meter Implementation Programme (SMIP) here run by the (former) Department of Energy and Climate Change (DECC), now BEIS,[118] with an installation target of 53 million gas and electricity smart meters across the UK by 2020. It is part of the wider EU shifts, namely the EU Third Energy Package[119] and specifically, Directive 2009/72/EC which requires 80% of Europe to be using smart meters by 2020. This means around 200 million electricity smart meters (72% of all European consumers) and 45 million gas meters.[120] SMIP has been delayed extensively with issues around cost, impacts on vulnerable populations and lacking transparency, to name a few.[121] Nevertheless, by 31 March 2016, official UK statistics show there are 2.75 million smart meters across UK operating in smart mode, representing 5.8% of total domestic meters in UK (DECC, 2016).[122]

At the consumer level, threats stem from smart meters and home energy management tools becoming compromised and exploited. Poorly secured IoT devices often use default passwords and thus have scope for data breaches as they interface with other IoT devices. This can lead to individual privacy harms, for example by compromised data directly or indirectly making patterns of daily life and occupancy visible to external actors. Smart thermostats and in-home displays to energy efficient smart lighting and washing machines share domestic networking, thus each can bring risks into the home. Another near future concern is security vulnerabilities in agent based systems deployed in the smart grid to assist with demand side management, e.g. with dynamic price tariffing. In the future, to level peak demands on the smart grid, prices may

[107] ENISA, "Smart Grid Security Recommendations" (Heraklion, 2015), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations.
[108] UN Office on Drugs and Crime 'Comprehensive Study on Cybercrime' (Vienna: UNODC 2013) p33.
[109] Giles Hogben (ed) *Botnets: Detection, Measurement, Disinfection and Defence* (Heraklion: ENISA 2013).
[110] See legal dimensions in Lilian Edwards "Dawn of the Death of Distributed Denial of Service: How to Kill Zombies", 2006, *Cardozo Arts and Entertainment Law Journal* 24(1), 23–59.
[111] Andy Greenberg, 'Summer of Discontent: Dragonfly 2.0 Hacking Campaign Targeted US and European Power Grids', *Wired*, 2017, https://www.wired.co.uk/article/hackers-power-grids-uk-symantec.
[112] Using Avalanche v3.6 program.
[113] The emails were made to appear to come from a manager within the company.
[114] Amended by Police and Justice Act 2006 s36.
[115] See s17(8)(b) CMA on definition of an 'unauthorised act'.
[116] *DPP v Lennon* [2006] EWHC 1201 (Admin) at 14.
[117] from Article 2 Energy Efficiency Directive (2012/27/EU).
[118] UK Department for Business Energy and Industrial Strategy.
[119] Electricity Directive (2009/72/EC) Annex I.2.
[120] European Commission, "Benchmarking Smart Metering Deployment in the EU 27 with a Focus on Electricity" (Brussels, 2014).
[121] Public Accounts Committee, "Twelfth Report: Update on Preparations for Smart Metering" (London, 2014).
[122] Meters operated by big energy firms e.g. British Gas, SSE, E. On etc.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

be changed rapidly to encourage consumption at different times. Due to complexity of managing this, consumers may need software agents negotiating tariffs on their behalf.[123] Compromised agents could create substantial energy bills for consumers, and again, be another forum for ransom and extortion, e.g. pay us £500 or pay a £750 energy bill.

The compromised IoT infrastructure, much like more traditional 'zombie PCs', can be implicated in botnets, particularly unsecured consumer grade systems. The Shodan search engine shows unsecured IP connected devices, like baby cams,[124] and the UK NCA argues, "the Shodan search engine reveals, for example, over 41,000 units of one insecure model of DVR are connected to the Internet as of January 2017".[125] These are being exploited, and recent DDoS attacks on a domain name service (DNS) company were mediated, in part, by the Mirai IoT botnet made up of compromised IP connected security cameras and digital video recorders (DVRs).[126] In 2017, more IoT botnets were found, including one targeting IP Cameras specifically, Persirai,[127] an IoT worm Hajime[128] and the Reaper botnet, created by actively hacking software instead of just hunting for default passwords.[129]

2.3.3.1. *Tackling botnets*. In fighting botnets, strategy argued by ENISA is to prevent new infections, break up existing botnets and minimise financial gains made from them.[130] These new IoT botnets are covered by the Council of Europe's longstanding Cybercrime Convention 2001 (CCC '01). IoT devices are computer systems within CCC '01's definition i.e. 'any device or group of interconnected or related devices, on or more of which, pursuant to a program, performs automatic processing of data'.[131] By way of background, it seeks to create "a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation".[132] It looks for harmonisation by signatories providing domestic legislation on five offences, including hacking, computer based fraud or distributing illegal content.[133] As of March 2017, it has 52 overall ratifications. The UK signed in 2001, ratified in 2011 and satisfies requirements through amendments to the Computer Misuse Act 1990. [134]

The relevance of CCC '01 has been questioned, primarily due to aging definitions and classifications of offences not encapsulating current attacks (like ransomware)[135]. In keeping it up to date, the Cybercrime Convention Committee (T-CY) has issued guidance notes[136] and they state botnets fall within CCC '01 remit because "computers in botnets are used without consent and are used for criminal purposes and to cause major impact ".[137] Accordingly, they are covered by many provisions of CCC '01, such as Article 2 on illegal access (due to the malware creating the zombie for the botnet) and Article 4 on data interference (as it alters data and sometimes delete, damage, deteriorate or suppresses it).[138] Information sharing and computer early response teams (CERTS) have an important role to play tackling botnets. We discuss CERTs further below, but the UK CERT and CiSP[139] information sharing scheme have made progress fighting bots.[140]

3. New legal requirements

Against the technical threat backdrop, we also have a range of regulatory considerations to consider. Organisations providing critical infrastructure have an increasing role in addressing cybersecurity risks. A key challenge is balancing these legal obligations with the commercial drive towards the industrial IoT. The EU Network and Information Security (NIS) Directive 2016,[141] enforced from May 2018,[142] defines obligations by establishing minimum pan-EU harmonised standards. EU member states need to adopt national measures and implementation strategies, particularly for cross-border cooperation. A network of computer security incident response teams (CERTS) and a strategic cooperation group to bring states together to share information about attacks are two examples. Short term, the UK remains committed to the NIS Directive, but long term, the nature of future cooperation remains unsettled.[143]

[123] Tom A. Rodden et al., "At Home with the Agents," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems – CHI '13* (New York, New York, USA: ACM Press, 2013), 1173, doi:10.1145/2470654.2466152.

[124] JM Porip, 'How to Search the Internet of Things for Photos of Sleeping Babies', *Ars Technica*, 2016, https://arstechnica.co.uk/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/ .

[125] National Cyber Security Centre and National Crime Agency, "The Cyber Threat to UK Business."

[126] Ibid.

[127] John Leyden, "Another IoT Botnet Has Been Found Feasting on Vulnerable IP Cameras • The Register," *The Register*, 2017, https://www.theregister.co.uk/2017/05/10/persirai_iot_botnet/.

[128] Waylon Grange, "Hajime Worm Battles Mirai for Control of the Internet of Things," *Symantec*, 2017, https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things.

[129] Greenberg A (2017) The Reaper IoT Botnet Has Already Infected a Million Networks, Wired https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

[130] Jan Gassen, Elmar Gerhards-Padilla, and Peter Martini, 'Botnets: How to Fight the Ever-Growing Threat on a Technical Level' in Heli Tirmaa-Klaar et al., Botnets (Springer 2013). p34.

[131] Article 1 Cybercrime Convention.

[132] See Preamble of Cybercrime Convention.

[133] Chapter II Section 1.

[134] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VOztoKSJ.

[135] Weber and Studer, "Cybersecurity in the Internet of Things: Legal Aspects."

[136] Committee on Cybercrime Convention, 9th Plenary of the T-CY (2013) Guidance Notes 2–7.

[137] Committee on Cybercrime Convention, 8th Plenary (2013) https://rm.coe.int/16802e7132 p6.

[138] Committee on Cybercrime Convention 8th Plenary (2013) p7.

[139] UK Cyber Security Information Sharing Partnership – https://www.ncsc.gov.uk/cisp.

[140] Samantha A. Adams et al., "The Governance of Cybersecurity The Governance of Cybersecurity: A Comparative Quick Scan of Approaches in," 58–60.

[141] NIS Directive EU 2016/1148 (NIS).

[142] NIS Article 25.

[143] http://www.out-law.com/en/articles/2017/january/network-and-information-security-directive-will-be-implemented-in-the-uk-despite-brexit-vote-government-confirms/.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

3.1. NIS directive 2016: security of essential services

With NIS, EU member states need to identify the operators of 'essential services' in their territory, from across energy, transport, banking, financial markets and health sectors.[144] This includes bodies such as energy operators involved in supply, distribution and storage of natural resources (e.g. oil pipelines, refineries and rigs); transportation providers (e.g. air carriers, intelligent transport systems or traffic management); banking (e.g. credit institutions); financial trading (e.g. stock markets); and healthcare providers (e.g. hospitals or clinics).

Article 14 NIS states operators of essential services need to put in place appropriate, proportionate technical and organisational measures to address risks posed to systems, relative to the state of the art. They need to take measures to ensure continuity of service and prevent/minimise impacts of incidents. They also need to notify relevant authorities (e.g. a regulator or computer emergency response team),[145] without undue delay, about incidents that affect their ability to provide their services, including cross border dimensions. Number of users affected by disruption of the service, duration of incident and geographical spread of area affected by the incident should be considered. This information may be shared with other member states so they can respond too.

Curiously, it also extends to three specific digital services, online marketplaces, search engines, and most interestingly here, cloud computing services.[146] With the latter, similar provisions to Article 14 on technical and organisational measures exist in Article 16 NIS, but add that the following factors should also be taken into account: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards. For determining if an incident is substantial, duration and geographical spread remain. However, impact on economic and societal activities, extent of disruption, and number of users relying on their services to provide their own services also need to be reflected. With digital services, the public may be notified where necessary by authorities. Article 16 does not apply to micro and small businesses.[147] With both Article 14 and 16, member states need to make sure that there are appropriate regulatory powers (including setting penalties)[148] for authorities to enforce the rules.[149]

In criticising NIS, Weber argues that the nature of appropriate and proportionate technical and organisational measures (APTO) measures remains nebulous; the exemption for SMEs, hardware and software providers is too much, as it excludes many important actors from the law; and, given reputational harms associated with reporting breaches, implementation of mandatory breach notification requirements may be lacklustre (Weber, p726). We provide exploration of APTOs.

3.2. Computer emergency response teams[150]: managing IIoT vulnerabilities

Any growth of industrial IoT in critical infrastructure, needs to ensure it complies with these substantive requirements in NIS around risk mitigation and notification requirements. In the context of distributed IoT devices, this could be a tall order. At a strategic level, alongside NIS, both the UK/EU Cybersecurity Strategies[151] cite the importance of CERTs in quickly addressing cybersecurity risks. Hence, at a societal level, in conjunction with ENISA, CERTs have a key role in training exercises, issuing guidance, and ensuring cooperation across borders for industrial IoT. Raising awareness and finding strategies to address nascent security risks will be a key role in the future.

Patching industrial IoT vulnerabilities is likely to be a huge undertaking, even if resources and planning are invested. The UK Cybersecurity Strategy argues that vulnerabilities are growing due to the number of systems going online, creating more threat vectors but poor cyber hygiene practices by the population, such as not using antivirus software, the lack of security skills across society, from the general-public to public and private sectors and also the continued use of unpatched legacy IT systems are primary concern.[152] The UK National Crime Agency echo the latter point, concerned that despite widespread publicity of many vulnerabilities, like Heartbleed, they have not been fully patched and remain.[153] This enables nation states to take advantage of the old vulnerabilities, utilising less sophisticated approaches to leverage hacks to steal intellectual property or state secrets, and leaving more sophisticated tools for when truly necessary.[154] How these vulnerabilities manifest in industrial IoT contexts remains to be seen.

3.3. EU general data protection regulation 2016: notification requirements and workers' personal data

The new EU General Data Protection Regulation 2016 (GDPR) also needs to be considered here as it includes provisions on security of personal data.[155] It includes new notification rules around personal data breaches i.e. 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[156] Any data controllers who suffer a personal data breach needs to notify the UK data protection regulator, the UK ICO, within 72 hours of discovery of the attack.[157] They need to provide quite detailed information in a very short period of time, *including*:

a) "the nature of the personal data breach including where possible, the categories and approximate number of data

[144] NIS Annex II.
[145] Called computer security incident response teams (CSIRTS) in NIS.
[146] NIS Annex III.
[147] Art 16(11) NIS Directive.
[148] NIS Article 21.
[149] NIS Articles 15 and 17.
[150] See NIS Article 9 for more on CSIRTS.
[151] Ian Levy, Active Cyber Defence – Tackling Cyber Attacks in the UK, NCSC, 2016 https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk.
[152] Government, "National Cyber Security Strategy 2016–2021."
[153] National Cyber Security Centre and National Crime Agency, "The Cyber Threat to UK Business," 9.
[154] Ibid., 7.
[155] GDPR Article 32.
[156] GDPR Article 4(12).
[157] GDPR Article 33.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

subjects concerned and the categories and approximate number of personal data records concerned.
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effect."[158]

In addition, they need to let the data subject know about the breach too, in a clear and plain manner, without undue delay (but not within 72 hours) is likely to pose high risks to their rights and freedoms.[159] However, they do not need to do this, if the following three conditions are met:

(a) "the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."[160]

Given the differentiated notification provisions here, end users are often likely to be finding out about data breaches through news stories or public messages from companies more often,[161] as data breaches in 2016 were 45% higher than in 2014.[162] As discussed above, the insecurity in the domestic IoT interfaces with industrial IoT, insofar as it becomes part of botnets that are then used to attack critical infrastructure. Cloud service providers have extensive security obligations under NIS, and the design of many IoT systems is orientated towards sensing data then aggregating it in the cloud for analytics to provide contextually relevant service. So, when IoT products utilise cloud services when handling personal data, both NIS and GDPR obligations could come to the fore. In terms of putting in place NIS mandated organisational and technical measures to ensure security, coupled with notification obligations from GDPR, the case gets stronger for IoT systems to be designed in a manner where cloud storage is not the dominant approach. As mentioned above, local data storage and analytics would help organisations avoid a lot of these difficult compliance requirements and enable more controlled and sustainable security architecture too. Technologies like personal information management systems[163] are useful for protecting consumers' personal data, but they also have much to offer for industrial IoT too, in terms of providing confidentiality or limiting access to sensitive information. Hardware level trusted execution environments (i.e. a secure space on the chip) can also play a role in industrial IoT, attesting to identities of devices in widely distributed systems.[164]

Another relevant provision of GDPR for IIoT is Article 32 on security of processing. IIoT is primarily about integrating and tracking information at different points in goods or service supply chains, but workers are also a key part of this process. IIoT can disrupt their current work practices by introducing greater oversight by observing how they complete tasks, spotting inefficiencies and trying to increase productivity through automation, where possible. Worker personal data is manifest in the mix meaning information privacy obligations still need to be considered and how IIoT systems impact their rights.[165] In some jurisdictions, a combination of labour laws, unionisation and system design could tackle negative impacts of IIoT and automation, as occurred with the Scandinavian School of Participatory Design movement when IT was introduced into workplaces in the 1970s.[166] However, we focus here on a specific security provision in Article 32 GDPR that deals with 'security of processing'. Personal data of workers needs to be handled in a secure manner, but the shortcomings in IIoT security may see them implicated in data breaches and other privacy harms. To prevent this, IIoT deployments need to take stock of Article 32 GDPR. Broadly, it states appropriate 'technical and organisational measures' need to be taken by controllers and processors to protect rights and freedoms of data subjects. This has to take into consideration: the 'state of the art', 'costs of implementation', 'nature, scope, context and purposes of processing' and 'likelihood and severity' of risk to their rights. They give examples such as pseudonymising or encrypting data, testing the resilience, integrity, confidentiality and availability of processing systems, or restoring access and availability of data quickly after an incident. If they abide by codes of practice, that can be a demonstration of compliance. Article 32 again surfaces the need for technical and organisational measures, which is a turn to the technical community to play a critical role in regulating the risks. Alongside

[158] GDPR Article 33 (3).
[159] GDPR Article 34.
[160] GDPR Article 34(3).
[161] However, with the recent Uber breach, both the UK Information Commissioner Office and UK public found out through the press – https://www.out-law.com/en/articles/2017/november/ubers-data-breach-handling-provides-lessons-for-others-ahead-of-gdpr-says-expert/#.WhlyUB7OfLY.twitter.
[162] ENISA, "ENISA Threat Landscape Report 2016."
[163] Richard Mortier et al., "Personal Data Management with the Databox: What ' S Inside the Box?," 2016, doi:10.1145/3010079.3010082.
[164] Markku Kylänpää and Aarne Rantala, "Remote Attestation for Embedded Systems" (Springer, Cham, 2016), 79–92, doi:10.1007/978-3-319-40385-4_6.
[165] G Iachello and J Hong, "End User Privacy in Human Computer Interaction," JOUR, *Foundations and Trends in Human Computer Interaction* 1, no. 1 (2007): 1–137; Leysia Palen and Paul Dourish, "Unpacking "privacy" for a Networked World," in *Proceedings of the Conference on Human Factors in Computing Systems - CHI '03* (New York, New York, USA: ACM Press, 2003), 129, doi:10.1145/642611.642635.
[166] Christiane Floyd et al., "Out of Scandinavia: Alternative Approaches to Software Design and System Development," *Human-Computer Interaction* (L. Erlbaum Associates Inc., December 1, 1989), doi:10.1207/s15327051hci0404_1.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

technical requirements of creating functioning IIoT systems, such legal requirements increasingly need to be thought about in early stages of the system design process.[167] However, like with privacy by design, this is much easier said than done, and extensive work will be needed to both situate the role of developers and security engineers in regulation. Work is needed to support their efforts to embed compliance mechanisms in design, through translation of law into technically actionable measures or through new tools to better surface their obligations.[168]

4. Engineering the industrial IoT: appropriate technical and organisational measures

As we have seen above, law is increasingly focusing on the role of technical and organisational measures to address cybersecurity risks. This is both in NIS, for critical infrastructure providers or GDPR, for security of personal data. Accordingly, the law is bringing technical professionals to the fore, and there is a growing space for technical responses for IIoT security, to supplant legal approaches. We have already hinted towards the importance of distributed storage approaches above and a growing need for edge computing too.[169] The bandwidth and networking challenges of sending large volumes of data (e.g. from autonomous vehicles) from sensors to the cloud for central analytics mean conducting analytics locally and sending back results is increasingly attractive.[170]

In reflecting on these issues and considering routes redressing the risks stemming from IoT, established practices in IT architecture design could be considered. Examples could include:

- Keep data distributed, as opposed to centralising the data into one, more vulnerable central storage point.
- Keeping data encrypted both when stored and when being sent over networks.
- Keeping controls on access by third parties through white lists and credentialing.
- Using local storage and analytics, where the raw data does not leave the hardware, and any analytics can be run locally (with results relayed back to relevant stakeholders).

Returning to our example of Industrial IoT on oil platforms in Section 2, we now explore putting networked sensors into devices in more detail. On the platform, monitoring integrity of components like valves on blowout preventers, connectors on hoses or structure of derrick frames would be important to save on possible down time by spotting issues early and observing performance to schedule servicing or replacement. Accordingly, sensors may be installed to:

- Monitor sudden changes in temperature;
- Pipe pressure;
- Oil flow speed;
- Fatigue in components;
- Strength of joints in pipelines;
- Analysis of chemical composition of quality of oil etc.

Depending how these sensors are networked, and how vulnerable they are to attacks, this shift could create new threat vectors. Taking a few examples below, we pose a range of questions to consider:

4.1. *Networking approaches*

Existing network infrastructure on rigs for getting data back onshore, will be important, or at least from installed sensor devices to the rig. What costs might be associated with telecoms provision to transfer data in remote locations like the North Sea or Siberia? Will the system use networking approach will be used (e.g. star, mesh)? How secure will these be? What protocols will be used for networking? Ensuring encryption during transmission will be key, how much bandwidth is available for relaying information will dictate the granularity of data that can be sent? And how regularly?

4.2. *On-board storage capacity*

How often do the sensors need to be 'emptied', with associated costs for servicing by staff (e.g. divers if they are remotely on the seabed? Distributed nature of the IoT system could be beneficial from a security perspective, but only if done properly.

4.3. *Computational capabilities*

Design decisions about processing power on devices dictate scope for local analytics vs the need to send to the 'cloud' for analysis on servers with greater computational capacity. Power and battery life of sensors could be a problem too, as adding processors would drain power more quickly. These decisions could create new threat vectors, for example around cloud security for confidential data.

4.4. *Resilience of devices*

Temporal considerations are key, as the harshness of the environment may impact physical security of devices and sensors.

[167] Urquhart and Rodden, "New Directions in Information Technology Law: Learning from Human–computer Interaction"; M Dennedy, J Fox, and T Finneran, *Privacy Engineer's Manifesto*, JOUR (New York: Apress, 2014); Irit Hadar et al., "Privacy by Designers: Software Developers' Privacy Mindset," *Empirical Software Engineering*, April 30, 2017, 1–31, doi:10.1007/s10664-017-9517-1.

[168] George Danezis et al., "Privacy and Data Protection by Design – from Policy to Engineering," *European Network and Information Security Agency* (Heraklion, 2014); Ewa Luger et al., "Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process," JOUR, in *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, vol. 1, (2015), 457–66, doi:10.1145/2702123.2702142.

[169] Carmela Troncoso et al., "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments," *Proceedings on Privacy Enhancing Technologies* 2017, no. 4 (2017): 307–29, doi:10.1515/popets-2017-0052.

[170] Mortier et al., "Personal Data Management with the Databox: What ' S Inside the Box?"; Wenting Zheng et al., "Opaque: An Oblivious and Encrypted Distributed Analytics Platform," accessed November 30, 2017, https://people.eecs.berkeley.edu/~wzheng/opaque.pdf.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

In terms of software, ability to update and patch vulnerabilities in the code may be difficult too, if devices are hard to access e.g. deep underwater.

5. Conclusions and further work

As we have explored, the emergence of CBS, as encapsulated by the industrial IoT, can bring many new security vulnerabilities. The context of smart energy infrastructure, from resource exploration to energy consumption, helped us unpack some of the key challenges. Engineering dimensions around sensors are useful to reflect when analysing how regulatory frameworks might shape the nature of the industrial IoT. From a legal perspective, balancing the obligations in NIS with the desire for industrial IoT is one challenge, the need for guidance from CERTS and authorities on IoT is another. Ultimately, security requirements from NIS and GDPR around cloud may also prompt growth of alternative architectures for the industrial IoT. How these may manifest legally, commercially and technically is an area in need of further research. In going forward, there needs to be an increased focus on understanding the implications of the shift of infrastructure from offline to online; how to handle temporal dimensions of security; how best to address implementation gaps for best practice; and how to engage with the infrastructural complexity of critical systems. To conclude, we consider each in more detail in turn.

5.1. *From Offline to Online*

New risks and vulnerabilities arise from networking infrastructure that is traditionally 'offline' being put online, and automating industrial processes that may traditionally have greater human oversight. Current best practices may not translate when automated, as security implications of putting something online that was not formerly networked might not be fully anticipated.

5.2. *Temporality and security*

Planning and building security into goods and services requires motivation, oversight and forecasting of risk. Managing security over time is a complex variable to consider. The distributed nature of IoT being integrated at scale into critical, industrial infrastructure poses questions about effective longitudinal strategies. Ensuring data security considerations are reflected at different points in the IoT product life cycle are key to long term system resilience. Optimal management of legacy systems that may be forgotten, unpatched and original technology vendors have long gone out of business is difficult. Maintaining oversight and updating firmware on distributed industrial IoT systems in a systematic manner will be even harder than the existing logistical challenges faced for in-house IT systems. Furthermore, the temporality of organisational security practices needs reflection, as management changes, processes are less well enforced, assets are hired, sold or decommissioned (perhaps even to competitors).

5.3. *Implementation gap for best practice*

In guarding against these threats, finding best practices to secure systems is critical and whilst guidelines[171] might be emerging, implementation must catch up. In practice, it is likely there will be a period of coexistence between legacy systems and new IoT devices, as we see in the domestic IoT. Furthermore, skills gaps for employees could be a key vulnerability and securing IoT infrastructure requires creating systems that are usable for workers, and retraining to ensure they are used correctly.

5.4. *Managing infrastructural complexity*

Systematic approaches considering how best to build security into these systems need to contend with the interdependent, complex nature of industrial systems (e.g. energy, manufacturing, logistics). Even if one element of a system puts appropriate security safeguards in place, when interacting with systems lacking these, vulnerabilities can surface. Over the course of IoT system life cycles, flaws will emerge, but the complex interactions between IoT systems may complicate meaningful anticipation of any second order effects. Responsibility for maintaining oversight of security within systems may be tractable, but establishing responsibility for the points where they interact with other systems may be harder. However, these challenges need to be addressed to avoid the emergence of the internet of insecure industrial things.

Acknowledgement

This work was supported by the Engineering and Physical Sciences Research Council [grant number EP/M02315X/1].

REFERENCES

Accenture Technology. Driving Unconventional Growth through the Industrial Internet of Things; 2015. Available from https://www.accenture.com/gb-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf. [Accessed 6 December 2017].

Adams SA, Brokx M, Corte LD, Galič M, Kala K, Koops B-J, et al. The Governance of Cybersecurity The Governance of Cybersecurity: A Comparative Quick Scan of Approaches in. TILT Working Paper; 2015. Available from https://pure.uvt.nl/portal/files/8719741/TILT_Cybersecurity_Report_Final.pdf. [Accessed 6 December 2017].

Alexander D. U.S. Reserves Right to Meet Cyber Attack with Force | Reuters. Reuters; 2011. Available from http://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116. [Accessed 6 December 2017].

Alperovitch D. Revealed: Operation Shady RAT. White Paper; 2011. Available from https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf. [Accessed 6 December 2017].

[171] See maintained list of IoT Security and Privacy Guidelines on Schneier on Security Blog https://www.schneier.com/blog/archives/2017/02/security_and_pr.html.

Anastasi G, Antonelli M, Bechini A, Brienza S, D'Andrea E, De Guglielmo D, et al. Urban and Social Sensing for Sustainable Mobility in Smart Cities. In 2013 Sustainable Internet and ICT for Sustainability (SustainIT), 1–4. IEEE; 2013. doi:10.1109/SustainIT.2013.6685198.

Anderson R, Barton C, Bhöme R, Clayton R, Van Eeten M, Levi M, et al. Measuring the Cost of Cybercrime: A Workshop. Workshop on the Economics of Information Security (WEIS); 2012, 1–31. Available from http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf. [Accessed 6 December 2017].

Bilge L, Dumitras T. Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. Proceedings of the 2012 ACM Conference on Computer and Communications Security – CCS'12; 2012. 833–44. doi:10.1145/2382196.2382284.

Bundesregierung D. The New High-Tech Strategy; 2014.

Burgess M. When a Tanker Vanishes, All the Evidence Points to Russia | WIRED UK. Wired UK; 2017. Available from https://www.wired.co.uk/article/black-sea-ship-hacking-russia?utm_content=bufferc8256&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer. [Accessed 6 December 2017].

Carr J. Responsible Attribution: A Prerequisite for Accountability. The Tallinn Papers: A NATO CCD COE Publication on Strategic Cyber Security; 2014. Available from https://ccdcoe.org/sites/default/files/multimedia/pdf/TallinnPaperNo6Carr.pdf. [Accessed 6 December 2017].

Chanthadavong A. Rio Tinto Digs for Value in Data. ZDNet; 2015. Available from http://www.zdnet.com/article/rio-tinto-digs-for-value-in-data/. [Accessed 6 December 2017].

Clarke RA, Knake RK. Cyber War: The next Threat to National Security and What to Do about It. Ecco; 2010.

Craggs B, Rashid A. Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design. In Proceeding - 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems, SEsCPS 2017, 22–25; 2017. doi:10.1109/SEsCPS.2017.5.

Da Xu L, Senior Member, He W, Li S. Internet of Things in industries: A survey. IEEE Trans Industr Inform 2014;10(4):doi:10.1109/TII.2014.2300753.

Danezis G, Domingo-Ferrer J, Hansen M, Hoepman J-H, Métayer DL, Tirtea R, et al. Privacy and Data Protection by Design – from Policy to Engineering. European Network and Information Security Agency. Heraklion; 2014.

Dennedy M, Fox J, Finneran T. Privacy engineer's manifesto. New York: Apress; 2014.

Dinniss HH. Cyber warfare and the laws of war. Cyber warfare and the laws of war. Cambridge: Cambridge University Press; 2012. doi:10.1017/CBO9780511894527.

Edwards L. Wikileaks, DDOS and UK Criminal Law: The Key Issues | Practical Law. Practical Law Company; 2010. Available from https://content.next.westlaw.com/Document/If375d9dee81911e398db8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1. [Accessed 6 December 2017].

Edwards L. Privacy, security and data protection in smart cities. Eur Data Prot Law Rev 2016;2(1):28–58. doi:10.21552/EDPL/2016/1/6.

ENISA. Protecting Industrial Control Systems: Recommendations for Europe and Member States. Heraklion; 2011.

ENISA. Smart Grid Security Recommendations. Heraklion; 2015. Available from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations. [Accessed 6 December 2017].

ENISA. ENISA Threat Landscape Report 2016. Heraklion; 2017.

European Commission. Benchmarking Smart Metering Deployment in the EU 27 with a Focus on Electricity. Brussels; 2014.

Finkle J. Hacker Group in China Linked to Big Cyber Attacks: Symantec. Reuters; 2013.

Finkle J. J & J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking. Reuters; 2016. Available from http://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUKKCN12411L. [Accessed 6 December 2017].

Floyd C, Mehl W-M, Reisin F-M, Schmidt G, Wolf G. Out of Scandinavia: Alternative Approaches to Software Design and System Development. Human-Computer Interaction. L. Erlbaum Associates Inc.; 1989. doi:10.1207/s15327051hci0404_1.

GE, Accenture, Junewarren-Nickle's Energy Group. Opportunities and Challenges for Digital Oilfield Transformation; 2015. Available from https://www.accenture.com/t20151218T203100__w__/nl-en/_acnmedia/PDF-2/Accenture-Digital-Oilfield-Outlook-JWN-October-2015.pdf. [Accessed 6 December 2017].

Glomsvoll O, Bonenberg LK. GNSS jamming resilience for close to shore navigation in the Northern Sea. J Navig 2017;70(1):33–48. doi:10.1017/S0373463316000473.

Government HM. National Cyber Security Strategy 2016–2021; 2016. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed 6 December 2017].

Grange W. Hajime Worm Battles Mirai for Control of the Internet of Things. Symantec; 2017. Available from https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things. [Accessed 6 December 2017].

Greenberg A. Summer of Discontent: Dragonfly 2.0 Hacking Campaign Targeted US and European Power Grids. Wired; 2017. Available from https://www.wired.co.uk/article/hackers-power-grids-uk-symantec. [Accessed 6 December 2017].

Hadar I, Hasson T, Ayalon O, Toch E, Birnhack M, Sherman S, et al. Privacy by Designers: Software Developers' Privacy Mindset. Empirical Software Engineering; 2017, 1–31. doi:10.1007/s10664-017-9517-1.

Haddadi H, Howard H, Chaudhry A, Crowcroft J, Madhavapeddy A, Mortier R. Personal Data: Thinking Inside the Box. London/Cambridge; 2015. doi:10.7146/aahcc.v1i1.21312.

Huggler J. Robot Kills Man at Volkswagen Plant in Germany – Telegraph. The Telegraph; 2015. Available from http://www.telegraph.co.uk/news/worldnews/europe/germany/11712513/Robot-kills-man-at-Volkswagen-plant-in-Germany.html. [Accessed 6 December 2017].

Iachello G, Hong J. End user privacy in human computer interaction. JOUR. Foundations and Trends in Human Computer Interaction 2007;1(1):1–137.

Igure VM, Laughter SA, Williams RD. Security issues in SCADA networks. Comput Secur 2006;25(7):498–506. doi:10.1016/j.cose.2006.03.001.

Karanasiou AP. The changing face of protests in the digital age: on occupying cyberspace and Distributed-Denial-of-Services (DDoS) attacks. Int Rev Law Comput Tech 2014;28(1):98–113. doi:10.1080/13600869.2014.870638.

Klahr R, Amili S, Shah JN, Button M, Wang V. Cyber Security Breaches Survey 2016. London; 2016. doi:10.13140/RG.2.1.4332.6324.

Koerner B. Inside the OPM Hack, The Cyberattack That Shocked the US Government. Wired; 2016. Available from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/. [Accessed 6 December 2017].

Kraemer S, Carayon P, Clem J. Human and organizational factors in computer and information security: pathways to vulnerabilities. Comput Secur 2009;28(7):509–20. doi:10.1016/j.cose.2009.04.006.

Kylänpää M, Rantala A. Remote attestation for embedded systems. Cham: Springer; 2016. p. 79–92. doi:10.1007/978-3-319-40385-4_6.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

Lee EA. Cyber Physical Systems: Design Challenges. Technical Report No. UCB/EECS-2008-8; 2008. Available from http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html. [Accessed 6 December 2017].
Leyden J. Another IoT Botnet Has Been Found Feasting on Vulnerable IP Cameras • The Register. The Register; 2017a. Available from https://www.theregister.co.uk/2017/05/10/persirai_iot_botnet/. [Accessed 6 December 2017].
Leyden J. Move Over, Stuxnet: Industroyer Malware Linked to Kiev Blackouts • The Register. The Register; 2017b. Available from https://www.theregister.co.uk/2017/06/12/industroyer_malware/. [Accessed 6 December 2017].
Luger E, Urquhart L, Rodden T, Golembewski M. Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process. JOUR. In Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems, 1:457–66; 2015. doi:10.1145/2702123.2702142.
Millard CJ. Cloud computing law. Oxford: OUP; 2013. doi:10.1017/CBO9781107415324.004.
Mortier R, Zhao J, Crowcroft J, Wang L, Li Q, Crabtree A, et al. Personal Data Management with the Databox: What ' S Inside the Box?; 2016. doi:10.1145/3010079.3010082.
Murakami Wood D, Carter M. Power Down. Limn; 2017. Available from http://limn.it/power-down/?doing_wp_cron=1495448151.7596950531005859375000. [Accessed 6 December 2017].
Nakashima E, Warrick J. Stuxnet Was Work of U.S. and Israeli Experts, Officials Say – The Washington Post. The Washington Post; 2012. Available from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.9ee2a60c2170. [Accessed 6 December 2017].
National Cyber Security Centre, National Crime Agency. The Cyber Threat to UK Business. London; 2017. Available from http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file. [Accessed 6 December 2017].
NATO, CCD COE. Tallinn manual on the international law applicable to cyber warfare. Tallinn: Cambridge University Press; 2013.
NATO, CCD COE. Tallinn manual 2.0 on the international law applicable to cyber operations. 2nd ed. Tallinn: Cambridge University Press; 2017.
Newman LH. Medical Devices Are the Next Security Nightmare. Wired; 2017. Available from https://www.wired.com/2017/03/medical-devices-next-security-nightmare/. [Accessed 6 December 2017].
O'Halloran D, Kvochko E. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. World Economic Forum, no. January (2015): 40.
Olson P. We are anonymous: inside the hacker world of LulzSec, anonymous, and the global cyber insurgency. Back Bay Books; 2013.
Out-Law. The Network and Information Security Directive – Implications for the Energy Sector. Out-Law.com; 2017. Available from https://www.out-law.com/en/topics/tmt–sourcing/cybersecurity/the-network-and-information-security-directive–implications-for-the-energy-sector-/. [Accessed 6 December 2017].
Palen L, Dourish P. Unpacking "privacy" for a Networked World. In Proceedings of the Conference on Human Factors in Computing Systems – CHI '03, 129. New York, New York, USA: ACM Press; 2003. doi:10.1145/642611.642635.
Perelman B. Air Gap or Not, Why ICS/SCADA Networks Are at Risk | SecurityWeek.Com. Security Week; 2016. Available from http://www.securityweek.com/air-gap-or-not-why-icsscada-networks-are-risk. [Accessed 6 December 2017].
Portnoff RS, Lee LN, Egelman S, Mishra P, Leung D, Wagner D. Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights. Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems 1; 2015:1649–58. doi:10.1145/2702123.2702164.
Public Accounts Committee. Twelfth Report: Update on Preparations for Smart Metering. London; 2014.
Randazzo M, Keeney M, Kowalski E, Cappelli D, Moore A. Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. Software Engineering Institute; 2005. Available from http://repository.cmu.edu/sei/457. [Accessed 6 December 2017].
Rid T. Cyber war will not take place. Hurst & Company; 2013.
Rodden TA, Fischer JE, Pantidi N, Bachour K, Moran S. At Home with the Agents. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems – CHI '13, 1173. New York, New York, USA: ACM Press; 2013. doi:10.1145/2470654.2466152.
Rolls Royce. Autonomous Ships: The Next Steps. Rolls Royce; 2016. Available from http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/rr-ship-intel-aawa-8 pg.pdf. [Accessed 6 December 2017].
Sadeghi A-R, Wachsmann C, Waidner M. Security and Privacy Challenges in Industrial Internet of Things. In Proceedings of the 52nd Annual Design Automation Conference on – DAC '15, 1–6. New York, New York, USA: ACM Press; 2015. doi:10.1145/2744769.2747942.
SAE International. New SAE International Standard J3016. SAE International; 2016. doi:P141661.
Slaughter A, Bean G, Mittal A. The Internet of Things in the Oil and Gas Industry | Deloitte University Press. Deloitte Insights; 2015. Available from https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-oil-and-gas-industry.html. [Accessed 6 December 2017].
Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A. Guide to Industrial Control Systems (ICS) Security. NIST; 2015. doi:10.6028/NIST.SP.800-82r2.
Symantec. Smarter Security for Manufacturing in the Industry 4.0 Era; 2016. Available from https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf. [Accessed 6 December 2017].
The Economist. The World's Most Valuable Resource Is No Longer Oil, but Data. Economist; 2017. Available from https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource. [Accessed 6 December 2017].
The Guardian. Gary McKinnon Resource Page. The Guardian; 2017. Available from https://www.theguardian.com/world/gary-mckinnon. [Accessed 6 December 2017].
Thomson I. BBC's Micro:bit Turns out to Be an Excellent Drone Hijacking Tool • The Register. The Register; 2017. Available from https://www.theregister.co.uk/2017/07/29/bbcs_microbit_drone_hijacking_tool/. [Accessed 6 December 2017].
Troncoso C, Isaakidis M, Danezis G, Halpin H. Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments. Proceedings on Privacy Enhancing Technologies 2017, no. 4; 2017: 307–29. doi:10.1515/popets-2017-0052.
UN Office on Drugs and Crime. Comprehensive Study on Cybercrime. New York; 2013. Available from https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf. [Accessed 6 December 2017].
Urquhart L, Rodden T. New directions in information technology law: learning from human–computer interaction. Int Rev Law Comput Tech 2017;31(2):1–19.
Wall D. Cybercrime: The Transformation of Crime in the Information Age. Polity; 2007.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

Wall D, Williams M. Policing cybercrime: networked and social media technologies and the challenges for policing. Routeledge; 2014.
Wang S, Wan J, Li D, Zhang C. Implementing smart factory of industrie 4.0: an outlook. Int J Distrib Sens Netw 2016;12(1):3159805. doi:10.1155/2016/3159805.
Weber RH. Internet of things: privacy issues revisited. Comput Law Secur Rev 2015;31(5):618–27. doi:10.1016/j.clsr.2015.07.002.
Weber RH, Studer E. Cybersecurity in the internet of things: legal aspects. Comput Law Secur Rev 2016;32(5):715–28. doi:10.1016/j.clsr.2016.07.002.
Wootson C JrMost Cybersecurity Experts Are Worried about Russian Hackers. One Says: Look, a Squirrel! The Washington Post; 2016.
World Economic Forum / Accenture. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. Cologny; 2015. Available from http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf. [Accessed 6 December 2017].
Zetter K. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired; 2011.
Zetter K. Car Wash Hack Can Strike Vehicle, Trap Passengers, Douse Them With Water – Motherboard. Motherboard; 2017. Available from https://motherboard.vice.com/en_us/article/bjxe33/car-wash-hack-can-smash-vehicle-trap-passengers-douse-them-with-water. [Accessed 6 December 2017].
Zheng W, Dave A, Beekman JG, Popa RA, Gonzalez JE. Opaque: An Oblivious and Encrypted Distributed Analytics Platform. Available from https://people.eecs.berkeley.edu/~wzheng/opaque.pdf. [Accessed 6 December 2017]. [Accessed 30 November 2017].

Author Information

Dr Lachlan Urquhart, Research Fellow in Information Technology Law, Horizon, University of Nottingham.

Prof Derek McAuley, Director of Horizon and Professor of Digital Economy, Horizon, University of Nottingham.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004