Digital Twins

CYBERSECURITY PROSPECTS, PITFALLS & RECOMMENDATIONS

WASSIM SAMY AZZOUG
RENAN GADONI CANAAN
MD KHAIRUL ISLAM
CLARENCE SOKOLAMBE LAKPINI
MATT MALONE
CROSS SMALLEY
TIFFANY WOO
AND
DR DAVID MURAKAMI WOOD

Human-Centric Cybersecurity Partnership

HUMAN-CENTRIC CYBERSECURITY REPORT PROJECT

The 2022 Human-Centric Cybersecurity Report Project brought together postgraduate students from across Canada to work with our partners from both private industry and the public sector to produce reports looking at wicked cybersecurity problems through a transdisciplinary lens. This three volume series comprises the following reports

- Challenges of Virtual Trust: A Matter of Cooperation, Education, and Cybersecurity
- Digital Twins: Cyber Security Prospects, Pitfalls, and Recommendations
- Cybersecurity Through Human Behavior

ABOUT HC2P

The Human-Centric Cybersecurity Partnership (HC2P) is a transdisciplinary group of scholars, government, industry and not-for-profit partners that generate research and mobilize knowledge that will help create a safer, more secure, more democratic and more inclusive digital society.

ACKNOWLEDGMENTS

We would like to thank the Bank of Montreal (BMO), Bell Canada, the Standards Council of Canada (SCC), and Innovation, Science and Economic Development Canada (ISED) for their efforts in supporting this project.

Cover Art - Michael Joyce x Nathan Dumlao @unsplash.com x dream.ai

Page 22 Illustration - A girl meets her Digital Twin - Michael Joyce x nightcafe.studio

This publication contains illustrations from Public Domain or conditionally licenced works available from the New York Public Library, NASA and Unsplash.com.

Cite as: Wassim Samy Azzoug, W. S., Canaan, R. G., Islam, M. K., Lakpini, C. S. Malone, M., Smalley, C., Woo, T. & David Murakami Wood, D. (2022) *Digital Twins: Cyber Security Prospects, Pitfalls, and Recommendations*. Human-Centric Cybersecurity Partnership HC2P.

Dépôt légal, Bibliothèque et Archives nationales du Québec, 2022

ISBN: 978-1-7387249-1-8

The Human-Centric Cybersecurity Partnership is supported in part by funding from the Social Sciences and Humanities Research Council.

Social Sciences and Humanities Research Council of Canada

Conseil de recherches en sciences humaines du Canada

Canada

Contents

Digital Twins

CYBERSECURITY PROSPECTS, PITFALLS & RECOMMENDATION

Executive Summary

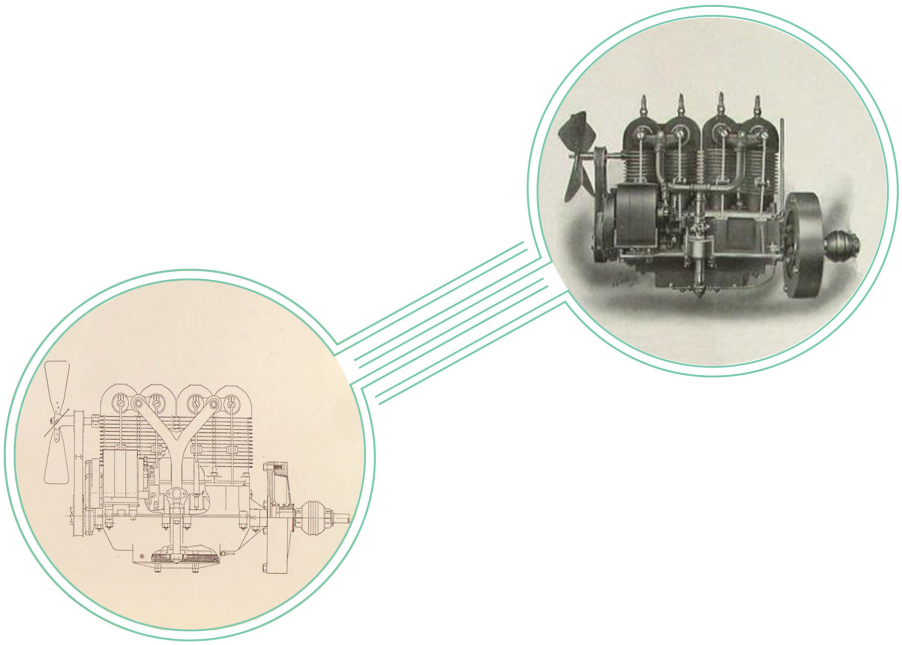
Digital twins, synchronized digital counterparts of a physical environment, are being extensively deployed in an array of new applications by government and private actors.

The technology offers:

- adaptiveness to monitor evolving ecosystems;
- to enable robust cybersecurity testing and analysis through simulation; and
- to allow stakeholders to deliver accurate, predictive results.

At the same time, the technology poses cybersecurity risks from:

- unintended and adversarial uses through potential compromises of data collection sensors and attacks on data integrity;
- new opportunities for intellectual property theft; and
- new vectors of attack on the integrity of cyber-infrastructure from vulnerabilities in data storage, systems, and software of digital twin technologies themselves.



Digital Twins — Synchronized Digital Counterparts of a Physical Environment

Recommendations

- To benefit from these advantages while addressing these concerns, stakeholders should design, develop, and deploy digital twins following the Gemini Principles and with an eye to interoperability.
- Government actors must adopt a human-centric and security-focused approach to digital twins, which places digital rights at the core.
- This approach must be coupled with:
  - strict controls on data collection meeting a necessity threshold;
  - strong data profiling parameters; and
  - augmented data breach and cybersecurity incident reporting requirements.
- Finally, stakeholders should put in place, monitor, and enforce the use of information security standards to thwart attacks premised on physical, data manipulation, software, data poisoning, and machine learning.

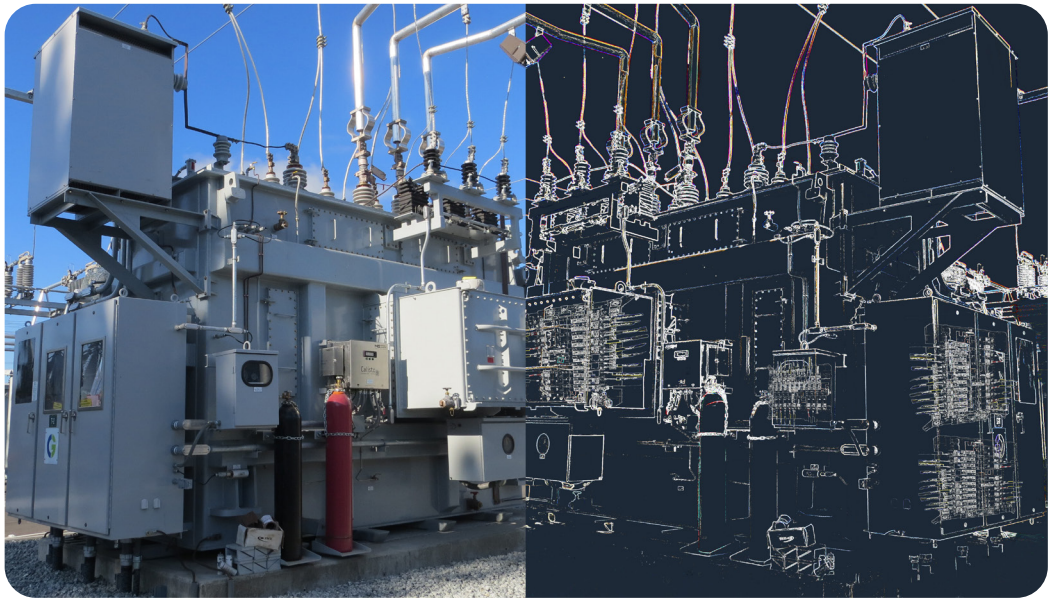
Introduction

1 Introduction and Project Scope

Digital twins, the synchronized digital counterparts of a physical environment, are being extensively used by government and private actors as a part of an evolving technology ecosystem. While they are providing benefits by enabling testing and analysis through simulation, the technology also poses cybersecurity risks.

This report reviews and analyses the prospects and pitfalls of the technology with a focus on the regulatory aspects of cybersecurity. It sets forth recommendations for next steps in cybersecurity regulation for the field. After a brief introduction providing an overview of the technology and its social, digital, and legal contexts, the report covers the following:

— **Part I** outlines the cybersecurity



Digital Twins - a Highly Complex Digital Replica connected to a Physical Entity by a Continuous Data Loop

promises of the technology, including its capabilities for adaptiveness, efficiency, proactiveness, and scalability.

— **Part II** outlines several potential cybersecurity pitfalls of the technology, including unintended and adversarial uses and the array of cyber threats they pose. It also examines pitfalls arising from legal and standardization uncertainty, in particular as they pertain to intellectual property rights; data privacy; social trust and legitimacy; bias and discrimination; and other equity issues.

— **Part III** outlines recommendations. It summarizes existing efforts to develop general standards and norms, like the Gemini Principles, ISO 23247, and interoperability proposals. It then discusses recommendations for digital rights, which include: ensuring robust data governance, tailoring necessary data collection, augmenting data breach reporting, and setting strong data profiling parameters. Finally, it sets out recommendations for the financial industry and specific technical countermeasures.

1.1 Concept of Digital Twins

Digital twin technology is the use of digital counterparts to provide a synchronous representation of a physical environment (Batty, 2018). At its core, the technology comprises a highly complex digital replica of a physical entity, featuring very detailed representations of real-world systems (Engstler, 2021; Eramo et al., 2021; National Research Council Canada (NRC), 2020). Some definitions of digital twins also include concepts, notions, and entities that are not just physical but also perceptual (Voas et al., 2021). The technology operates by collecting information from various inputs, such as gadgets and sensors, which it compiles into a centralized interface enabling manipulation and the provision of new insights to improve processes in a two-way dynamic coupling of the virtual and real worlds (Botín-Sanabria et al., 2022; da Silva Mendonça et al.,

2022).

The increasing use of digital twins raises many legal and ethical issues. This report examines regulatory aspects of digital twins as they relate to cybersecurity in Canada, particularly focusing on the non-technical aspects of such regulation. The authors were guided by several principles, including seeking to avoid duplication of scholarship and writing on legal and ethical applications of AI, prioritizing proactive (not retroactive) regulation, and approaching regulation as a broadly construed notion that includes norms and general standards, as well as law. Broadly understood, regulation is an essential part of the economy and society, underpinning markets, ensuring service delivery, and protecting consumers' rights and safety. Because digital twin technology remains largely unregulated, regulatory landscapes must continue to adapt and evolve. This report reviews and analyzes the technology's prospects and pitfalls from a cybersecurity perspective, and sets forth recommendations for next steps in the field of cybersecurity regulation.

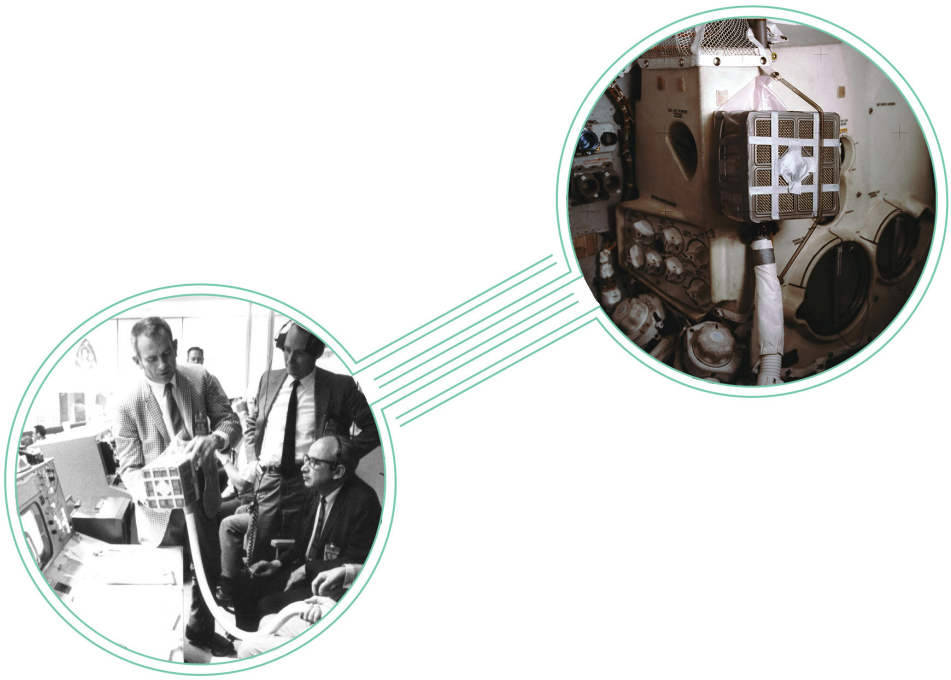
At first glance, the term digital twins can be misleading. Digital twins are more than simple copies of a physical object. A digital twin is a sophisticated virtual replica of a physical object. These software-based virtual representations of an object's life cycle or a system, are updated with real-time data and use simulation and machine learning (IBM, 2022). Digital twin technology realistically represents assets, processes, or systems from the built or natural environment in the digital realm. The cause-and-effect relationships modelled by digital twins can assist with real-world decision-making.

Central to digital twin technology is the notion of synchronicity. It is this aspect of digital twins that distinguishes them from other types of digital models due to their continuous and lasting connection to their physical counterpart through data-collecting hardware through an information and feedback loop (Bolton et al., 2018). They permit updating data "in real-time so that virtual models can improve continuously through data updates from physical assets" (Da Silva Mendonça et al., 2022, p. 2). Digital twins accumulate and interpret significant amounts of data from physical sources "to make predictions and or create simulations of how the physical object or system will react in the real world" as data is being added to alter the model itself (Elder, 2022; National Research Council Canada, 2020). Digital twins could be considered to be a nascent technology. Although they are not yet commonplace, digital twins have already been extensively used for digitally reproducing and improving large-scale processes in the aerospace industry (Miskinis, 2019) and are also gaining ground in the automated vehicle industry. Despite the limited use of the technology until this point, the potential for exponential growth is clear. Consequently, there remains a pressing need to understand the technology's prospects and challenges in the Canadian regulatory context across all industries and applications (Aitken, n.d.).

1.2 Social and Digital Context

1.2.1 Early History

The historical origins of digital twin technology can be traced back to NASA's space exploration



NASA linked Simulation Systems and the Apollo 13 Spacecraft with a Constant Data Loop in 1970

mission Apollo 13 in 1970 (Allen, 2021). During that mission, the explosion of an oxygen tank two days after the start of the mission forced NASA to problem solve remotely by mobilizing several simulation systems linked to a constant data loop with the damaged spacecraft; these simulation systems created a mirror of the spacecraft to resolve technical challenges and to bring the vessel and its passengers home safely (Ferguson, 2020).

1.2.2 Introduction of the Modern Term

The modern concept of digital twins was first publicly introduced in a presentation by Michael Grieves on 'product lifecycle management' (PLM) at the University of Michigan in 2003 (Tao et al., 2019). Dr. Grieves applied digital twin software technology to manufacturing industries in 2003. In 2010, NASA's John Vickers introduced 'Digital twin' as a new term (Grieves, 2019)

1.2.3 New Applications

The idea of replicating or 'scale modelling' of a physical object to modify, study, and develop physical objects is not new. However, the connection between the digital twins and the physical object distinguishes digital twins from other replica systems. What makes digital twins' cloning physical objects different is the realism of these replications and the speed at which they are synchronized. Due to this aspect of the technology, there are many cybersecurity applications imminent to the technology. For example, an *Emerging Technology Snapshot* prepared by the NRC notes that digital twins are "enabling a more proactive and predictive approach to the defence of digital data" (National Research Council Canada, 2020). When Digital Twins are combined with artificial intelligence, the advantages become even more evident. A key benefit of the

technology identified for digital twins is the way in which digital twin technology marshals artificial intelligence to "remove the barriers of interoperability between heterogeneous data" (Ferdousi et al., 2021, p. 2).

1.2.4 Sample Cases and Benefits

Digital twins are extensively used in an array of applications including power-generation equipment, critical infrastructure systems, manufacturing operations, healthcare services, the automotive industry, and urban planning. The use of human digital twins is still new, but it is likely to gain momentum with the popularization of "metaverse" systems (Nguyen, 2022). The technology's rapid evolution results in wide implementation of novel tech applications in both public and private sectors. Many countries are considering digital twin as a means of their socio-economic development, as outlined in greater detail in the case study "National Digital Twin Programmes".

1.2.5 North American Market Dominance

North America has an increasing market share in the digital twin industry. This is unsurprising, given the overlap between the development of digital twin technology with existing capacity in product design and development (Aashish, 2022). In terms of market valuation, it is estimated that the digital twins market will be worth $73.5 billion by 2027, with the North American region expected to dominate the market during this time (Aashish, 2022). One reason for this anticipated market capture is government efforts to provide tax incentives and special packages for manufacturing and infrastructure companies, which will contribute to advance the digital twin market in the region (Aashish, 2022). Currently, several industries are leading, in particular aerospace, automotive and transportation, energy, utilities, and food & beverage industries (IBM, 2022). Across these industries several companies have proposed data protection and cybersecurity standards for digital twins in their sector

1.1.1 Case Study: National Digital Twin Programmes

Several countries have recently developed national digital twin programmes. Grenada, Singapore, Luxembourg, and Britain have either started development or have instituted a complete national digital twin programme (Walters, 2019). The British effort, the National Digital Twin programme (Ndigital twinsp), was initiated in July 2018 and is operated by the Centre for Digital Built Britain (Walters, 2019). This operation is a partnership between the University of Cambridge and the Federal Departments for Business, Energy, and Industrial Strategy (Walters, 2019). The core purpose of the initial effort was to provide insight into the National Infrastructure Commission's 2017 Data for the Public Good Report (Walters, 2019). In addition to providing a specific digital twin tailored to data analytics, the Ndigital twinsp has also focused on creating an information management framework to connect future digital twins in specific industries, such as industrial manufacturing and the construction of built environments (Walters, 2019). The development of national programs has been justified through the potential creation of social, economic, commercial, and environmental benefits (Walters, 2019).

(Winkle, 2021).

1.3 Current Regulatory and Legal Framework

Currently, there is no standalone statute or regulatory or legal framework in Canada that directly governs digital twins. Nonetheless, human-centered digital twins have a direct relationship with data associated with a natural person. Digital twins draw on aggregated personal data to derive information and knowledge. Therefore, the core of digital twins comprise data, algorithms and AI systems (Teller, 2021). As such, as with any digital service that collects and uses personal information, they are subject to existing Canadian cybersecurity, privacy, and data protection statutes and regulations. Here, we explore the interaction between the digital twins and these current legal frameworks.

1.3.1 Privacy Act

Government institutions in Canada are subject to regulation with respect to the collection, retention, and use of the personal information of individuals under the Canadian *Privacy Act*. The *Privacy Act* stipulates that government institutions shall collect personal information only if it "*relates directly* to an operating program or activity of the institution" (emphasis added) (Privacy Act, 1985, sec. 4). Government institutions must abide by stringent rules when utilizing data for purposes other than those identified at the time of collection and when disclosing personal information under their control (Privacy Act, 1985, sec. 7). Individuals also have the right to access their retained information upon request (Privacy Act, 1985, sec. 12(1)).

Although the *Privacy Act* is a central component to Canada's overall legal framework for privacy protection, the *Act* in its current form is inadequate for protecting information in the digital age. Concerns with the *Privacy Act* include, but are not limited to, frustration with the low standard for data collection ("relates directly" instead of a higher standard of necessity), weak forms of informed consent for novel uses of collected personal information, and a lack of private enforcement combined with strained resources of public enforcement bodies. Efforts to modernize the *Act* are ongoing, with the Department of Justice having recently launched an online public consultation to obtain feedback from Canadians on how to update the *Act* (Department of Justice 2022). A modernized *Privacy Act* will have implications for the management of personal data by federal institutions, including data collected for digital twins.

1.3.2 The Personal Information Protection and Electronic Documents Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) is perhaps the most impactful privacy and data protection statute in Canada. PIPEDA is the federal statute that regulates the collection, use, and disclosure of personal information by federally regulated and private sector organizations in the course of commercial activities (Canada, 2018). Provinces that do not have analogous privacy and data protection legislation use the PIPEDA framework, which is only pre-

empted in provinces with substantially similar or more stringent frameworks (Act Respecting the Protection of Personal Information in the Private Sector, 2021; Personal Information Protection Act, 2003a; Personal Information Protection Act, 2003b).

According to PIPEDA, organizations subject to the Act must take measures to avoid theft, loss, disclosure, modification, use, or unauthorized access to personal data from customers and employees (PIPEDA, 2000 art. 4.7.1) and adhere to basic security safeguards, which are defined in Schedule 1 of the Act (PIPEDA, 2000 sch. 1). Federally regulated companies are required to designate an officer to be responsible for complying with the Act's provisions (PIPEDA, 2000 art. 4.1). Companies should also take steps to secure personal data protection, such as using encryption (PIPEDA, 2000 art. 4.7.3).

This will remain the case for the design, development, and deployment of digital twin technology. In the absence of statutes or regulations directly governing digital twins, the safeguards in PIPEDA will assume great significance for private actors deploying the technology. The required security safeguards and the basic measures in PIPEDA will serve as a baseline for the cybersecurity standards of personal data stored in digital twin systems used by private actors. However, given PIPEDA came into force over two decades ago, the framework's design from a different technological era is likely to struggle to achieve the aspirational safeguards it sets out.

1.3.3 The Office of the Superintendent of Financial Institutions (OSFI)

The Office of the Superintendent of Financial Institutions (OSFI) exercises additional governance over the cybersecurity measures of Federally Regulated Financial Institutions (FRFIs). The OSFI's mandate is to supervise FRFIs and assist them in developing risk-management frameworks (Office of the Superintendent of Financial Institutions [OSFI], 2013). The OSFI's approach to cybersecurity is principles-based, permitting it to be tailored to specific financial institutions, depending on factors like their size and complexity. In 2013, the OSFI launched a cybersecurity self-assessment tool that enables FRFIs to assess their level of cyber preparedness and implement best cybersecurity practices (OSFI, 2013). This self-assessment has rating levels (1-to-5) to help financial institutions gauge the security controls of their digital systems, including digital twins (OSFI, 2013). In July 2022, OSFI released new guidelines for technology and cyber risk, balancing innovation with risk management, that will enter into effect on January 1, 2024. These new guidelines will likely be useful in supporting the continued advancement of digital twin technology.

1.3.4 Criminal Code

The Canadian *Criminal Code* (1985) contains several provisions that may be pertinent to digital twins, in particular in a deterrent capacity in responding to cybersecurity incidents. For example, section 342.1 (unauthorized use of computer) and section 391 (fraudulent obtainment of trade secrets) may serve as springboards for law enforcement to crackdown on

cybersecurity breaches of digital twin platforms. At present, provisions relating to property are unlikely to have much effect, given the precedent established in Canadian law that does not recognize confidential information as property within the context of theft (*R. v. Stewart*, 1988). This precedent is likely to remain in force. It should also be noted that the deterrent effect of criminal law as a means of channelling and shaping cybersecurity norms will be determined to a certain degree by the level and sophistication of enforcement. The Public Prosecution Service of Canada (PPSC), which prosecutes offences on behalf of the Government of Canada, has no sections devoted exclusively to cybercrime or intellectual property theft. Without such resources, there remain important questions about government capacity to address problems involving digital twins where criminal issues arise.

1.3.5 Other Human Rights Frameworks

It is almost certain that digital twin technology might raise novel questions relating to certain rights under the *Charter* (1982). For example, if public bodies engage in decision-making on the basis of digital twin technology, they may engage certain *Charter* rights, such as the right to liberty and security of a person. The use of a digital twin of an individual to make a decision on behalf of an individual might deprive the individual of certain degrees of personal autonomy and decision making. Likewise, private bodies who use digital twin technology for workforce decisions would do so against the backdrop of relevant human rights commissions. Given the inherent fluidity of rights frameworks, public and private bodies using the technology are likely to encounter rights' based challenges to their practice.

1.4 Proposed Cybersecurity Legislation

In addition to these established regulatory frameworks, there are newly proposed developments regarding cybersecurity regulation in Canada that may impact the regulation of digital twins from a cybersecurity standpoint. As part of its National Cyber Security Strategy, the federal government proposed Bill C-11, a *Digital Charter* (Innovation, Science and Economic Development Canada, 2022) with 10 principles, including a "safety and security" principle (Innovation, Science and Economic Development Canada, 2022). These principles were intended to guide policy making in relation to developments in the digital economy, including the emergence of digital twins across industries (Innovation, Science and Economic Development Canada, 2022). However, Bill C-11 did not become law and died on order paper in 2021 as the result of the federal election (*Digital Charter Implementation Act*, 2021). In June 2022, the federal government reintroduced the *Digital Charter Implementation Act* (Bill C-27) to strengthen privacy and data protection laws and create new rules for responsible AI. Bill C-27 is a revised iteration of Bill C-11. It contains three provisions: (1) the *Consumer Privacy Protection Act*, (2) the *Personal Information and Data Protection Tribunal Act*, and (3) the *Artificial Intelligence and Data Act* (Innovation, Science and Economic Development Canada, 2022). If passed into law, the Consumer Privacy Protection Act will replace PIPEDA (Innovation, Science and Eco-

nomic Development Canada, 2022). Given the uncertainty of these legislative efforts, their direct effect on digital twin technology use by private and public actors will need further observation and study.

To further bolster Canada's cybersecurity posture, the federal government also recently introduced Bill C-26, (*An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts*, 2022). In addition to imposing various cybersecurity obligations on such actors, this proposed legislation has introduced the *Critical Cyber Systems Protection Act*, which seeks to help organizations better prevent and respond to cyber incidents (*An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts*, 2022). Bill C-26 could strengthen cybersecurity across numerous sectors including financial, energy, telecommunications, and transportation. For example, Bill C-26—or a similar legislative or regulatory effort—could create proactive duties to offer design resilience and fault-tolerance. Authorization and auditing to meet baseline cybersecurity standards may be necessary by a third-party regulatory body when it comes to the deployment of digital twin technology.

1.1.1 Case Study: Data Protection and Cybersecurity Compliance in Urban Digital Twins

DUET (Digital Urban European Twins) is a company that develops smart-city digital twins and has already worked with many cities in Europe. To address legal concerns regarding data privacy and cybersecurity, DUET has linked its digital twin system with personal data owners (i.e., citizens), allowing them to self-determine the consent on the use of their data for any purpose. Also, DUET has implemented security measures at various levels of its system: at the fringe (at the level of the sensors that send data to the system), at the core (the cloud-based platform that treats all data received from the fringe), and at the communication paths that connect both (Raes et al., 2022).

Part I Promises

2 Promises of Digital Twins

This part examines the promises of the technology, in particular its adaptability, efficiency, proactiveness, and scalability.

2.1 Adaptability

Digital twins offer agility in the form of quick responsiveness to ecosystem changes. This permits the technology to adapt to fast-changing regulations, in a world where product development consists of processes that never finish (Tung et al., 2020). A core aspect of the technology is its incorporation of real-time data. This has made it particularly attractive to organizations operating large complex sys-

1.1.1 Case Study:

In farming and agriculture, digital twin technology can permit more effective remote data collection, thereby addressing challenges otherwise presented by labour shortages. For example, Mojow Autonomous Solutions Inc., an Alberta-based company, has proposed using sensors that create and update a digital twin representation of field-level issues (Agriculture and Agri-Food Canada, 2022).

tems, including the Royal Canadian Navy and the Royal Canadian Air Force (Renaud et al., 2020). In the smart city context, real-time information collected, harvested, and scraped from sensors permits continuous improvement of efficiency in urban spaces at lower costs and through reduced use of resources (Botín-Sanabria et al., 2022).

2.2 Efficiency

With new technologies such as the Internet of Things (IoT), key cybersecurity risks rest in the lack of standardization of software creating multiple vectors of attack. Digital twins provide the opportunity to use a standard representation for such technologies in "multiple use cases such as [common vulnerability and exposure] scanning, zero-day analysis and detecting privacy violations" (Engstler, 2021). Likewise, software developers are reluctant to share source code input in light of concerns around misappropriation of trade secrets and confidential information and infringement of patent and copyright intellectual property. The use of digital twin technology permits developers to "share critical information about their products without having to worry about the integrity of their IP" (Voas et al., 2021). It also permits the testing of processes without presenting disruptions to those processes themselves, which, in turn, could "shake up supply chains" (The Economist, 2017).

2.3 Proactiveness

Digital twins offer an approach to cybersecurity that is proactive. As the National Research Council of Canada notes, digital twins for novel digital networks can "simulate attack scenarios and pinpoint vulnerabilities before the system is even implemented" (National Research Council Canada, 2020). In advance of cyber attacks, the technology may permit business and government actors to better assess and calculate risk. In the event of a cyberattack itself, digital twin technology could serve a business continuity function in providing "a full accounting of assets and network data mapping" (Choi, n.d.).

In this regard, digital twins may become a significant prong in the defense of critical cyber infrastructure, serving as a useful complement to legislative efforts to bolster such systems. For example, Bill C-26 introduced in the 1st Session of the 44th Parliament requires covered entities to "identify and manage any organizational cyber security risks, including risks associated with the designated operator's supply chain and its use of third-party products and services" (*An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts*, 2022). This helps shift the

1.1.1 Case Study:

On Friday 8th July 2022, millions of Customers of Rogers Communications, one of the biggest telecom companies in Canada were left without telephone and internet services for roughly 15 hours. The breakdown not only inconvenienced users but affected essential services such as healthcare facilities, 9-1-1 services, and financial services (The Canadian Press, 2022). According to the CEO, the outage was caused by a system failure which happened during the maintenance of the core network (The Canadian Press, 2022). The emergence of digital twin technologies may permit companies like Rogers to take anticipatory steps by employing the technology to monitor and optimise their core operation, mitigating such breakdowns to bolster and sustain more resilient systems (Faleiro et al., 2022).

cybersecurity paradigm from one that conceptualizes such threats retroactively to one that identifies and addresses them proactively.

2.4 Scalability

Digital twins enhance the large-scale collection and manipulation of data to deliver predictive results for complex environments. It is noted that digital twins can be used to fight problems for which we currently have scale challenges, including climate change and pandemics (Botín-Sanabria et al., 2022; National Research Council Canada, 2020). At ETH Zürich, computer scientists and climate scientists have developed a digital twin of the earth to test “climate science and meteorological aspects of the Earth’s digital twin” (Ulmer, 2021). The use of modeling permits better management of complex systems whose scale otherwise renders them unmanageable.

1.1.1 Case Study:

Replica is an American company spun off from Google’s sibling Sidewalk Labs, which develops urban digital twins through an approach that gathers information from millions of users from different decentralized datasets. Replica’s digital twin allows for assessing the “big picture” of the built environment as well as the impact of decisions in urban areas. The product provides city planners with insights into transit conditions, such as origin-destination flows, latent demands, and biking and pedestrian patterns. Replica has already worked with large cities such as Chicago, New York, and Sacramento (Replica, n.d.).

Part II Potential Pitfalls

3 Potential Pitfalls of Digital Twins

This part outlines several potential pitfalls of the technology, including unintended and adversarial uses posed by an array of cyber threats. It also examines pitfalls arising from legal and standardization uncertainties, in particular as they pertain to intellectual property rights, data privacy, social trust and legitimacy, bias and discrimination, and other equity issues.

A failure to regulate the digital twin market could pose threats to the human and non-human subjects being replicated. Left unregulated, digital twin technology may pose threats to safety, privacy, data protection, intellectual property, and other types of risks identified below. To grasp the concerns about failure to regulate, it is essential to understand the na-

ture of these risks.

3.1 Unintended and Adversarial Risks

One of the greatest promises of digital twin technology is also its greatest weakness, centralization. Digital twin technology relies on a vast array of inputs to permit real-world operation by capturing network power channelling those inputs into a platform for their manipulation and control (Voas et al., 2021). Because digital twin technology "centralizes sensitive data and control interfaces," it provides tremendous power to parties in control of the technology, such as the companies building, providing, or creating the software for such interfaces. Unfortunately, this also increases access in the event of a hack (Voas et al., 2021). Breaches of this interface can provide significant opportunity to create harm within the digital twin ecosystem. Even slight alterations to the representation of the digital twin, if fed back out to the sensors from the digital interface, can create immediate real-world effects; alternatively, it can permit "remote control" of the real-world objects (Voas et al., 2021). Another type of adversarial use of the technology comes from the manipulation of the sensors themselves; in effect, feeding malicious, incorrect, unreliable, or faulty inputs to the sensor in order to mislead, confuse, or disrupt the digital interface itself.

Threats stemming from unintended and adversarial uses include the following types:

3.1.1 Physical Threats

While the physical security of IoT devices is important, they can be damaged, destroyed, or even stolen by attackers. Due to their connection with physical components, digital twins systems have different priorities than typical network or system security needs (Humayed et al., 2017). For instance, because the technology is linked directly to a physical environment, severe product flaws could result in fatalities, serious injuries, or environmental harm. Safety must therefore be seen as the most important security need. Safety can be characterized as the prevention of damage or hazard to the physical environment infrastructure that could result from system vulnerabilities (Lu et al., 2015).

3.1.2 Data Modification Threats

Even if a digital twin system uses hardware that is both tamper-proof and tamper-resistant to prevent data change, data modification by the attacker is still conceivable. Data alteration can be carried out by data poisoning attacks or by taking advantage of flaws in the system, software, or data connectivity.

3.1.3 System Threats

Digital twin software is a virtual layer within a complex system which is also subject to having cybersecurity vulnerabilities. Digital twin system software will generally be run on top of an operating system that manages the server hardware and other applications. Flaws in this operating system could be exploited by an attacker to take complete control of the digital twin programme or to obtain a copy of it. The digital twin provides value by providing services to other applications, such as those providing data analysis or system con-

trol functions. Malicious applications could be designed to exploit the digital twin system, potentially launching any of a wide range attacks. In digital twin-based smart manufacturing systems, these attacks could lead to a total denial of service and significant losses. Additionally, industrial control and operating systems could be attacked by malware (Branquinho, 2017).

3.1.4 Software Threats

Unauthorized access to the source code or software of the digital twin, which serves as the blueprint for the actual system, might have serious consequences. As a result, an attacker might be able to assess the system and identify its weaknesses. The attacker might then succeed in breaking into the back-end systems as well (Hearn & Rix, 2019).

Intellectual property and company secrets may be threatened if an attacker can obtain access to the digital twin software's beta version (or precious source code). Weak software protection could be caused by poor coding. Attackers can employ reverse engineering techniques to get the system's source code if the programme is poorly protected or not protected at all (Krotofil & Gollmann, 2013).

3.1.5 Intellectual Property Theft Threats

A digital twin includes intellectual property, which may be subject to infringement and misappropriation. Because digital twins are models of physical objects, they can be used as a digital model of crucial business assets. Often, they represent an actual system or object so closely that if the twin is accessed, it can serve as a blueprint to the physical object itself. Such conduct will open new opportunities for intellectual property infringement and misappropriation. For example, if the digital twin is a blueprint of a given intellectual property, then malicious actors may be able to reverse engineer and reproduce that property from the digital twin itself.

3.1.6 Data Storage Threats

Cloud computing services are the primary data storage platform for digital twin applications. Data that is stored is delicate and subject to numerous dangers. Data leaks will happen if cloud computing is breached. Because digital twin technology aims to represent its physical counterpart as accurately as possible, it is a repository for enormous amounts of data. Consequently, human and non-human data can be used for the digital twins of physical objects. Digital twin technology raises the possibility of the collected data revealing sensitive information about individuals' life and behavioural patterns. If someone can gain access to the digital twin, they could not only get insights into the system, but also—more dangerously—get control of those physical assets. This can result in uncontrollable behaviours (Thorpe, n.d.). Information can lose its integrity when people are able to access it and make unauthorized changes. To ensure your information maintains its integrity, proper authentication and security measures must be in place to prevent unwanted modifications (Thorpe, n.d.).

3.2 Legal and Standardization Uncertainties

Expansion in the use of digital twins will create many novel questions regarding law and standardization. At present, there is "no standardized approach to digital twin modelling, resulting in various levels of performance, reliability, security and interoperability" (National Research Council Canada, 2020; Voas et al., 2021). This lack of standards is recognized as a key factor inhibiting wider-scale adoptions of digital twin technologies (Botín-Sanabria et al., 2022). Along with this lack of infrastructure, there is a risk that legislators and policy-makers will not adapt quickly enough in responding to the new risks and challenges created by digital twins. There is a subsidiary possibility of "standards blending" occurring, as a global, comprehensive, accepted, and entrenched set of standards comes into place (Voas et al., 2021). Given this lack of laws and standardization, several key legal questions remain unanswered in the context of digital twins.

3.3 Intellectual Property Rights

In addition to these adversarial concerns identified above, the creation of a digital twin, even prior to its initial utilization, necessitates the creation of a digitized product. Ownership over the product becomes a question of growing complexity, with more stakeholders involved in the project (Lesley et al., 2021). Copyright and trademark regulations are also likely to become significant areas of concern as perennial issues of these areas of intellectual property law are engaged by the technology. For all forms of intellectual property, a key concern will be the role of exceptions, including public interest exceptions. It is important to note that at the time of writing, there are no regulations explicitly governing the ownership of data within a digital twin system (Faleiro et al., 2022).

3.4 Data Privacy

Issues related to the control and extent of personal information collected about digital twins will mirror in importance ongoing conversations about privacy and data protection in digital realms. Because digital twins collect such a significant amount of data, if a data aggregator is able to package this data into extensive profiles of individuals, digital twin technology will create and provide significant insights about people. Control will become a significant concern for individuals (and for their loved ones upon the passing of those individuals). Obtaining meaningfully informed and ongoing "consent" to use data from private individuals will pose a significant question for the use of the technology, since much of the data will likely be scraped in a manner that bears little resemblance to future manipulations and applications of the data in a digital twin technology use. Jurisdictional legislation surrounding individuals' data privacy, including the variation in privacy and data protection laws around the world reflecting different levels of concern for such issues, will also influence the use of digital twins (Margaret, 2022).

A Girl meets her Digital Twin

3.5 Social Trust and Legitimacy

Using designations of trade secrets and confidential information to avoid disclosure of technology in the context of public-private partnerships is already widespread. For example, Innovation, Science, and Economic Development, maintains the Pan-Canadian AI Strategy, that was invoked in response to access to information requests exemptions for trade secrecy, confidential information, and information prejudicial to competitive position in an average of 23 percent of all requests it processed between 2011 and 2020. In 2019-2020 alone, Public Services and Procurement Canada did so in 41 percent of all requests it processed. In 2020-2021, that number jumped to 45 percent of all requests it processed (Malone, 2022, p. 4). These statistics point to a trend in government that is widespread and not specific to any particular department, ministry, or agency.

In the context of data collection by public entities, forcible data collection, retention, and use must be matched with proper regard for accountability and transparency (Malone, 2022). One of the risks that arises from the deployment of digital twin technology is how stakeholders may provide insufficient access to information, transparency, or accountability. Such conduct may impact the legitimacy (or perceived legitimacy) of institutions deploying the technology. Scoping the limits around what type of data collection is permissible will be an important task with such considerations in mind. Indeed, the transparency and accountability of digital twin systems may be challenged by the involvement of private sector actors working in collaboration with the public sector to deliver critical services, in particular

if those actors remain insistent on business models favouring opacity and non-transparency. In public-private partnerships, these dynamics will challenge the ability of existing legislation to provide transparency and accountability. This remains a challenge that access to information and freedom of information frameworks will face in balancing cybersecurity needs with proper regulatory oversight.

3.6 Bias and Discrimination

Digital twin technology's intricate relationship with artificial intelligence will clarify existing concerns around the production of bias and unjust outcomes being visited on vulnerable groups. Efforts to thwart such outcomes in the Canadian context, such as the Directive on Automated Decision-Making and its mandatory algorithmic impact assessments, will need to be augmented and tailored directly to these threats in the context of digital twins. Otherwise, the types of documented concerns around bias and discrimination in all types of contexts (public and private) and all types of kinds (racial, gender, sexual minority, etc.) will go unmitigated (e.g., an algorithm used by Amazon to draft product descriptions that resulted in the creation of a racist description for a children's toy) (Barrera, 2021). These are all issues that will be augmented by digital twin technologies.

3.7 Other Equity Issues

The costs of implementing digital twin technology are significant. The dependence on accelerated and deeply-connected networks means that regions with high rates of connectivity will benefit from the technology, while regions with reduced connectivity will avail themselves of less of these benefits. Due to their reliance on real-time sensors and IoT resources, the availability of digital twin technology will be constrained in countries with lower rates of connectivity and sensor technology infrastructure. This will almost necessarily create adoption challenges in developing countries (Botín-Sanabria et al., 2022). This problem taps into the "digital divide" in the capacity to use technology, which traverses other cleavages like age, geography, education (access to skills and training), facility in certain languages, and jurisdictional boundaries. While hardware challenges pose limitations on deployment, software and skills challenges will create knock-on effects and ongoing barriers to effective implementation (Botín-Sanabria et al., 2022). Overcoming these barriers may incentivize public-private models based on a "data for technology" (Wylie, 2020). This in itself presents cybersecurity concerns by perpetuating systematic problems in reducing bargaining power.

In November 2020, the Government of Canada made ArriveCAN mandatory for all travelers entering the country. In February 2021, it did so for all travelers. The smartphone app utilizes an artificial intelligence optical character recognition algorithm that is designated a trade secret (Treasury Board of Canada Secretariat, n.d.). In the wake of this secrecy and nondisclosure, ArriveCAN has been beset with problems, such as incorrectly "glitching" and sending faulty quarantine orders to 10,200 people (Hill 2022). In turn, such errors matched with a lack of transparency and accountability have led the app to become the subject of far-right and conspiratorial thinking that has captivated social media (Maxime Bernier [@MaximeBernier], 2022).

Part III Recommendations

4 Recommendations

This Part outlines recommendations. It summarizes existing efforts to develop general standards and norms, like the Gemini Principles, ISO 23247, and interoperability proposals. These standards and norms provide a strong foundation to prevent stifling technological innovation with restrictive laws through general standards. Adhering to these frameworks is an important initial step for public and private actors in adapting to codified forms of regulation that will eventually replace them, along with developing “made in Canada” models.

4.1 General Standards and Norms

4.1.1 The Gemini Principles

In 2018, the Centre for Digital Built Britain at Cambridge University published its guiding paper on the Gemini Principles. The Centre describes the Gemini principles as a series of nine foundational values that ensure the cultivation and utilization of 'data for the public good' (Bolton et al., 2018). If used correctly, they are intended to establish aligned principles across the materially built environment and to contribute to a broader framework for the development of digital twins in a variety of environments (Bolton et al., 2018). The principles break down into three primary categories: purpose, trustworthiness, and effective functionality. The first of these categories, 'purpose' is broken into values concerning the public good; value creation; and insight. The second category of 'trust' emphasizes the protection of data security. Poor quality data can potentially compromise the legitimacy of the digital twins and corrupt the insights gained from it. The final category, 'function', emphasizes selecting a standard federated and/or connected environment that can be observed, has a well-curated environment and which permits evolution over time (Bolton et al., 2018). These established principles are transferable to other Commonwealth jurisdictions that prioritize similar ethical values in both public and private spheres. Building upon the standard from "Digital Built Britain," Canada can develop a model that addresses uniquely Canadian values and issues.

4.1.2 International Organization for Standardization

The International Organization for Standardization (ISO) is a network of national standards bodies, which includes Canada. ISO is developing standards for virtual representations of the physical world, including developing a digital twin manufacturing network standard. ISO has developed ISO 23247 ("Digital twin framework for manufacturing"), which "defines a framework to support the creation of digital twins of observable manufacturing elements including personnel, equipment, materials, manufacturing processes, facilities, environment, products, and supporting documents." It comprises four components, including one each for general principles, architecture, information attributes, and technical requirements (ISO, 2021). However, to date, it has not released the general principles to the public.

4.1.3 Interoperability

Digital twins are systems of systems, being composed of different equipment and devices, each system connected to other engineering systems and devices. To benefit the most from these digital twins systems, prioritizing interoperability is essential to permit new connections and data flows to feed different systems, permitting the extraction of more value from the aggregated data (Lawton, 2022). Prioritizing interoperability has already emerged as a significant issue in combating the concentration of market power in the hands of social media platforms and large technology companies hoarding data. In the context of digital twins, it will continue to gain

1.1.1 Case Study: Interoperability and cybersecurity standards in the built environment sector

ARUP is a transnational Engineering Consulting company based in London, which develops digital twins for a sustainable built environment. To avoid market barriers such as customers' mistrust and lack of data interoperability in the built environment sector, ARUP has proposed seven principles for digital-twin companies in the built sector: (1) security; (2) data encryption; (3) identity and authentication; (4) the principle of least privilege; (5) security audits; (6) monitoring live events, and responding to incidents, (7) management of devices (ARUP, 2019).

importance. In this regard, current efforts to push interoperability of systems, such as the European Union's Digital Markets Act, will have a profound impact on the development of digital twins technology.

4.2 Recommendations for Government Actors

In Canada, government data collection, retention, and use operates within a different normative and legal framework than the same actions done by private actors. This raises concerns that are unique to government actors, in particular in the context of mandatory collection, retention, and use or where such conduct occurs in the absence of informed consent. For example, the application of Charter protections to government conduct invites recourse to its protection against that conduct.

4.2.1 Protecting Digital Rights

The growing concerns for security including, but not limited to, public safety, and strict regulations to protect the environment, as well as workplace and personal safety warrant a human-centric and security-focused approach to digital twins. However, the scope and impact of digital twin technology on the lives of citizens by public and private actors remains largely unknown. One may claim that current and recent legal frameworks, such as data protection and AI regulations address these concerns, securing rights for individuals and imposing duties on data processors (Teller, 2021). Current legal frameworks allow individuals to track what is done with their data and control data processing, but only to the extent that the individual is conscious of the impacts of his or her decision. In Canada, those frameworks, such as PIPEDA and the Privacy Act, rely on people's ability and will to exercise their rights.

Nonetheless, digital twins may raise questions beyond awareness and will. Digital twins can be used to unconsciously influence people's conduct and influence an individual's control over his behaviour (Teller, 2021). Private and public city planners may use personal data embedded in digital replicas to predict behaviour and prescribe solutions to urban policies that shape citizen behaviour (Wang and Burdon, 2021), such as relying on citizens' traffic information to shape the policy on the use of streets. Although they will have a great impact on how citizens behave, these automated decisions are undertaken as a black box because they do not allow the participation and insights of the subjects (Green, 2019).

To adapt the legal system to these new challenges arising from a digitalized world, activists have claimed the introduction of new fundamental rights entitled "meta-rights" (Murray & Fussey, 2019). They consist of the right to know the reasons behind actions designed by algorithmic decisions (right to be informed), the right to forget and be forgotten in the digitalized environment (right to be forgotten) and the right to disobey the behaviour designed by software and automated decisions (right to disobey).

4.2.2 Ensuring Robust Data Governance

To maintain the maximum level of privacy, user-specific data governance policies must be implemented in governmental uses of digital twins. Prior to selecting a technology and adhering to certain standards, it is crucial to have a comprehensive understanding of the needs (Thorpe, n.d.). A solid data management plan must be in place to ensure that these policies are properly applied. Such a plan would determine who is in charge of the data at various stages of its lifetime, such as data engineers, analysts, stewards, or business analysts. The access management, data reaction, and data residency criteria for each dataset and role must be determined. These requirements must be met at all stages of the data's lifecycle, including when it is being ingested, when it is at rest (i.e., not being utilized), when it is being transferred, and when it is being computed. Crucial data governance processes like masking, redaction, differential privacy, encryption, and lifecycle management should be implemented with the aid of a variety of solutions. Additionally, frameworks and rules must be in place to guarantee that data is shared securely, and with sufficient quality to provide real value.

4.2.3 Using Necessary Collection

As a general matter, security requirements must be dictated by the needs of a given digital twin technology. It will be important to define the purpose of a technology very clearly, by articulating specific uses that are

Case Study: TWINN - Digital Twin For Financial Institutions

The Singaporean AI start-up Precipient has launched the first digital twin applied to financial service institutions. Their product, called "TWINN", aims at accelerating the digital transformation of financial service institutions without requiring radical hardware updates. With TWINN, the digital twin is applied to the legacy system (i.e. outdated hardware) in what is called a "use-what-you-have" approach. The digital twin encompasses the whole banking sector, from infrastructure to customer service. TWINN allows for optimizing processes related to immediate customer onboarding. In a recent trial in an unamed Middle Eastern bank, new customers onboarded in a contactless fashion, and received a credit limit in a few minutes, just using a QR code (Digital Finance, 2020). TWINN also provides instant insights into customers such as price discounts and marketing analytics based on purchases, past searches and digital interactions (Percipient, n.d.). The digital twin is deemed to be applied to the API Exchange (APIX), an online Global FinTech Marketplace and Sandbox platform for banks and insurance companies in developing countries created by the Monetary Authority of Singapore and the International Finance Corporation (a private sector arm of the World Bank).

driven by an understanding of the information and control the end-users require. Given the inevitable challenge that use of the technology will pose to informed consent, parties using the technology should be held to a necessity standard. In other words, parties should be held to a standard to collect only the data they truly need. Adhering to this principle will facilitate defining user-specific data governance and management strategies for the technology (Thorpe, n.d.).

4.2.4 Employing Strong Data Profiling Parameters

Digital twin technologies must identify and classify the data sources. Critical metrics and regulatory standards should be allocated to each dataset as part of this data profiling activity. Engaging in this activity requires asking some key questions, such as 'Is this dataset publicly or privately owned?', 'Which license does it fall under?', 'Which part of the dataset needs to be anonymized?', 'If data is not available, how can we generate it?', and 'How do we transfer data between systems in a secure way?' (Thorpe, n.d.). Such questions will help guide the ultimate profiling of the data, and, following its profiling, its assignment to standards of varying degrees of intensity (e.g., low-impact cybersecurity concerns versus high-impact cyber security concerns.) This would mirror the Government of Canada's Algorithmic Impact Assessment Tool that determines risk attenuation needs by assigning a risk level to the algorithms.

4.2.5 Augmenting Data Breach Reporting

Since digital twins rely on data collected from varied sources, previously siloed public and private data may swirl together in the mix of a digital twin model. The purpose of data silos is to keep information private and save data from falling into the hands of unauthorized users. Likewise, in the case of a breach, data can completely leave the control and possession of a private or public entity. Breaches affecting government institutions are already significantly rising; for example, government institutions reported 250 material privacy breaches in 2020-21 (Treasury Board Secretariat 2021). In this regard, requirements around reporting data breaches will continue to be a significant tool.

4.3 Recommendations for the Financial Industry

The use of digital twins may allow for cost reductions by optimizing processes in the financial industry. For example, the data collected from customers' flow in bank branches could allow for branch traffic simulation, leading to rethinking branch layout to improve traffic flow and increasing social distancing (Comas, 2020). Furthermore, the financial industry is quickly adopting digital transformation and digital banking to become the first choice for financial services. Therefore, to avoid customers' mistrust in such virtual operations, digital twins could be used to increase the cybersecurity of financial transactions. Digital twins could run simulations of cyberattacks in order to improve system cybersecurity robustness (Tung et al., 2020). This is of paramount importance since new and more innovative methods of cyberattack are developing at a fast pace.

4.4 Relevant Technical Measures

In Part II, we outlined several unintended and adversarial threats that exist. Although it is not the scope of this paper to provide a complete list of technical countermeasures to resist such threats and risks, here we briefly outline technical countermeasures:

4.4.1 Physical Attack Countermeasures

Ensuring the security of gadgets and sensors that collect and scrape data for digital twins is paramount. The likelihood of insider threats may be reduced by putting information security concepts into practice, such as establishing access restrictions and granting as few privileges to the physical entities related to digital twins as possible (Karaarslan & Babiker, 2021).

4.4.2 Data Manipulation Countermeasures

Parties seeking to counterattack possible data manipulation threats should consider deploying technologies like IPFS, blockchain, hash functions, and similar technologies that can be utilized to ensure data integrity (Karaarslan & Babiker, 2021).

4.4.3 Software Attack Countermeasures

Following best practices in hardening operating systems is likely to exclude some critical attack vectors. The majority of software flaws and vulnerabilities will be guarded against by a secure software development cycle (SDLC). To stop software piracy and system reverse engineering, security testing should be used, and robust defences can be put in place. Additionally, patch management, periodic updates, and penetration testing are crucial in preventing many vulnerabilities. These efforts will aid in reducing hazards associated with software (Karaarslan & Babiker, 2021).

4.4.4 Data Driven Attack Countermeasures

Cloud computing serves as the primary data storage platform for digital twin applications. Data that is stored is delicate and subject to numerous dangers. Data leaks will happen after cloud computing is breached. Data storage raises a number of trust and privacy concerns, particularly when using a public cloud where the service provider firm has total authority.

We observe an increase in the use of technologies like IPFS (Interplanetary file system) and distributed file systems can also be used to store the data (Karaarslan & Babiker, 2021). However, we suggest that we shouldn't only rely on new technologies to maintain the digital twins' integrity. It is important to identify necessary security and compliance requirements and any existing controls, to select your cloud provider, service, and deployment models. As well as defining the architecture, assessing the security controls, identifying and implementing controls to control gaps remains important (CSA, 2022).

5 References

Aashish, M. (2022, July 19). Digital Twin market worth $73.5 billion by 2027. MarketsandMarkets. https://www.marketsandmarkets.com/PressReleases/digital-twin.asp

Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 (2021).

Agriculture and Agri-Food Canada. (2022, April 5). Government of Canada invests in digitization of farming to strengthen sustainability of Canada's Agriculture Sector. Government of Canada. https://www.canada.ca/en/agriculture-agri-food/news/2022/04/government-of-canada-invests-in-digitization-of-farming-to-strengthen-sustainability-of-canadas-agriculture-sector.html

Aitken, A. (n.d.). Industry 4.0: Demystifying Digital Twins. Lanner. https://www.lanner.com/assets/User/2511-Industry4.0_Demystifying_the_Digital_Twin.pdf

Allen, B. D. (2021, November 1). Digital Twins and Living Models at NASA. Digital Twin Summit, United States. https://ntrs.nasa.gov/citations/20210023699

An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 1st Session, 44th Parliament, Bill C-26 (2022).

An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts. (2021). [Historical information]. Parliament of Canada. https://www.parl.ca/legisinfo/en/bill/43-2/c-11

ARUP. (2019). Digital Twin: Towards a meaningful framework. https://www.arup.com/en/perspectives/publications/research/section/digital-twin-towards-a-meaningful-framework

Balkin, J. M. (2018). Free speech is a triangle. Columbia Law Review, 118(7), 2011–2056.

Barrera, Jorge and Albert Leung. (May 17, 2021). AI has a racism problem, but fixing it is complicated, say experts. https://www.cbc.ca/news/science/artificial-intelligence-racism-bias-1.6027150.

Bolton, A., Butler, L., Dabson, I., Enzer, M., Evans, M., Fenemore, T., Harradence, F., Keaney, E., Kemp, A., Luck, A., Pawsey, N., Saville, S., Schooling, J., Sharp, M., Smith, T., Tennison, J., Whyte, J., Wilson, A., & Makri, C. (2018). Gemini Principles ((CDBB_REP_006)). Centre for Digital Built Britain. https://doi.org/10.17863/CAM.32260

Botín-Sanabria, D. M., Mihaita, A.-S., Peimbert-García, R. E., Ramírez-Moreno, M. A., Ramírez-Mendoza, R. A., & Lozoya-Santos, J. de J. (2022). Digital Twin Technology challenges and applications: A comprehensive review. Remote Sensing, 14(6), 1335. https://doi.org/10.3390/rs14061335

Branquinho, M. A. (2017). Ransomware in industrial control systems. What comes after Wannacry and Petya global attacks? 329–334. https://doi.org/10.2495/SAFE170301

Canada, O. of the P. C. of. (2018, January 9). PIPEDA in brief. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Canadian Charter of Rights and Freedoms, S 8, Part 1 of the Constitution Act 1982, being

Schedule B to the Canada Act 1982 (UK), 1982, c11 (1982).

Choi, B. Q. (n.d.). How to avoid paying a ransom. Booz Allen Hamilton. Retrieved July 27, 2022, from https://www.boozallen.com/markets/commercial-solutions/how-to-avoid-paying-a-ransom.html

Comas, A. (2020, October 27). Building smarter banking branches with Digital Twins. Microsoft in Business Blogs. https://cloudblogs.microsoft.com/industry-blog/microsoft-in-business/financial-services/2020/10/27/building-smarter-banking-branches-with-digital-twins/

Criminal Code, R.S.C., 1985, c. C-46 (1985).

da Silva Mendonça, R., de Oliveira Lins, S., de Bessa, I. V., de Carvalho Ayres, F. A., de Medeiros, R. L. P., & de Lucena, V. F. (2022). Digital Twin Applications: A survey of recent advances and challenges. Processes, 10(4), 744–755. https://doi.org/10.3390/pr10040744

CSA (2022) Cloud Security Alliance Guidance for Critical Areas of Focus in Cloud Computing. https://cloudsecurityalliance.org/research/guidance/

Department of Justice. (March 7, 2022). Modernizing Canada's Privacy Act – Engaging with Canadians. https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/index.html#:~:text=As%20part%20of%20its%20commitment,the%20Act%20can%20be%20updated,

Digital Finance. (2020, July 12). Percipient "changing how banks change." https://www.digfingroup.com/percipient/

Elder, J. (2022, June 16). 'Digital Twins' manage the airport and hospitals. Are people next? San Francisco Examiner. https://www.sfexaminer.com/archives/digital-twins-manage-the-airport-and-hospitals-are-people-next/article_830b8d84-37b7-502c-a06c-f245f93cf899.html

Engstler, M. (2021, February 25). The Cyber Digital Twin revolution. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/02/25/the-cyber-digital-twin-revolution/

Faleiro, R., Pan, L., Pokhrel, S. R., & Doss, R. (2022). Digital Twin for cybersecurity: Towards enhancing cyber resilience. In W. Xiang, F. Han, & T. K. Phan (Eds.), Broadband Communications, Networks, and Systems (Vol. 413, pp. 57–76). Springer International Publishing. https://doi.org/10.1007/978-3-030-93479-8_4

Ferdousi, R., Laamarti, F., Hossain, M., Yang, C., & El Saddik, A. (2021). Digital Twins for well-being: An overview. Digital Twin, 1, 7. https://doi.org/10.12688/digitaltwin.17475.1

Ferguson, S. (2020, April 14). Apollo 13: The first Digital Twin. Siemens. https://blogs.sw.siemens.com/simcenter/apollo-13-the-first-digital-twin/

Google. (n.d.). How Content ID works. YouTube Help. Retrieved August 1, 2022, from https://support.google.com/youtube/answer/2797370?hl=en

Green, B. (2019). The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future. https://doi.org/10.7551/mitpress/11555.001.0001

Grieves, M. W. (2019). Virtually Intelligent Product Systems: Digital and Physical Twins. In S. Flumerfelt, K. G. Schwartz, D. Mavris, & S. Briceno (Eds.), Complex Systems Engineering: Theory and Practice (pp. 175–200). American Institute of Aeronautics and Astronautics, Inc. https://doi.org/10.2514/5.9781624105654.0175.0200

Hearn, M., & Rix, S. (2019). Cybersecurity considerations for Digital Twin implementations. IIC Journal of Innovation, 107–113.

Hill, Brian. (August 11, 2022). Experts warn ArriveCAN app could be violating constitutionally protected rights. https://globalnews.ca/news/9047177/experts-warn-arrivecan-app-could-be-violating-constitutionally-protected-rights/

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A survey. IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

IBM. (2022, July 20). What is a Digital Twin? https://www.ibm.com/topics/what-is-a-digital-twin

Innovation, Science and Economic Development Canada. (2022, June 16). Canada's Digital Charter: Trust in a digital world. Government of Canada; Innovation, Science and Economic Development Canada. https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

ISO. (2021, January). Automation systems and integration—Digital twin framework for manufacturing—Part 1: Overview and general principles. https://www.iso.org/obp/ui/#iso:std:iso:23247:-1:ed-1:v1:en

Karaarslan, E., & Babiker, M. (2021). Digital Twin security threats and countermeasures: An introduction. 2021 International Conference on Information Security and Cryptology (ISCTURKEY), 7–11. https://doi.org/10.1109/ISCTURKEY53027.2021.9654360

Lawton, G. (2022, May 27). Emerging Digital Twins standards promote interoperability. VentureBeat. https://venturebeat.com/2022/05/27/emerging-digital-twins-standards-promote-interoperability/

Lesley, S., Simon, B., Michael, C., Melissa, F., Andrew, H., Tim, G., & Sheila, M. (2021, August 7). What are Digital Twins and what are the legal issues with them? Gilbert+Tobin Law. https://www.lexology.com/library/detail.aspx?g=d-da9e40b-f8ed-4ee0-96ea-4848711dd4c2

Lu, T., Lin, J., Zhao, L., Li, Y., & Peng, Y. (2015). A security architecture in Cyber-Physical Systems: Security theories, analysis, simulation and application fields. International Journal of Security and Its Applications, 9(7), 1–16.

Malone, M. (2022). Third party record exemptions in Canada's Access to Information Act. Centre for International Governance Innovation, 172, 18.

Margaret, M. (2022, April 20). Legal issues and Digital Twins. Aviationpros. https://www.aviationpros.com/airports/article/21264787/legal-issues-and-digital-twins

Maxime Bernier [@MaximeBernier]. (2022, August 6). The ArriveCan app is a pilot test for a digital identification program in partnership with the WEF. https://t.co/UNQIosoNiv [Tweet]. Twitter. https://twitter.com/MaximeBernier/status/1555913242907709440

Miskinis, C. (2019, January). Future role of Digital Twins in the Aerospace Industry. Challenge Advisory. https://www.challenge.org/insights/digital-twin-in-aerospace/

Murray, D., & Fussey, P. (2019). Bulk surveillance in the Digital Age: Rethinking the Human Rights Law approach to bulk monitoring of Communications Data. Israel Law Review, 52(1), 31–60. https://doi.org/10.1017/S0021223718000304

National Research Council Canada. (2020). Emerging technology snapshot: Digital Twins. Public Services and Procurement Canada Government of Canada. https://publications.gc.ca/site/eng/9.902196/publication.html

Nguyen, T. N. (2022). Toward Human Digital Twins for Cybersecurity Simulations on the Metaverse: Ontological and Network Science Approach. JMIRx Med, 3(2), e33502. https://doi.org/10.2196/33502

Office of the Superintendent of Financial Institutions. (2013, October 25). Cyber Security Self-Assessment. Government of Canada. https://www.osfi-bsif.gc.ca:443/Eng/fi-if/in-ai/Pages/cbrsk.aspx

Percipient. (n.d.). Overview. Retrieved August 1, 2022, from http://www.percipientcx.com/products/

Personal Information Protection Act, SA 2003, c P-6.5 (2003).

Personal Information Protection Act, SBC 2003, c 63 (2003).

Privacy Act, R.S.C., 1985, c. P-21 (1985).

R. v. Stewart, 1 SCR 963 ___ (SCC 1988). https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/331/index.do

Raes, L., Michiels, P., Adolphi, T., Tampere, C., Dalianis, A., McAleer, S., & Kogut, P. (2022). DUET: A framework for building interoperable and trusted Digital Twins of Smart Cities. IEEE Internet Computing, 26(3), 43–50. https://doi.org/10.1109/MIC.2021.3060962

Renaud, G., Liao, M., & Bombardier, Y. (2020). Demonstration of an Airframe Digital Twin Framework using a CF-188 Full-Scale Component Test. In A. Niepokolczycki & J. Komorowski (Eds.), ICAF 2019 – Structural Integrity in the Age of Additive Manufacturing (pp. 176–186). Springer International Publishing. https://doi.org/10.1007/978-3-030-21503-3_14

Replica. (n.d.). About Replica. Retrieved August 3, 2022, from https://replicahq.com/about/

Tao, F., Qi, Q., Wang, L., & Nee, A. Y. C. (2019). Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and comparison. Engineering, 5(4), 653–661. https://doi.org/10.1016/j.eng.2019.01.014

Teller, M. (2021). Legal aspects related to Digital Twin. Philosophical Transactions of the Royal Society A, 379(2207), 20210023. https://doi.org/10.1098/rsta.2021.0023

The Canadian Press. (2022, July 9). Rogers CEO apologizes for massive service outage, blames maintenance update. CBC News. https://www.cbc.ca/news/business/rogers-outage-interac-debit-restored-1.6515869

The Economist. (2017, July 13). Millions of things will soon have Digital Twins. The Economist. https://www.economist.com/business/2017/07/13/millions-of-things-will-soon-have-digital-twins

The Personal Information Protection and Electronic Documents Act, S.C., c. 5 (2000).

Thorpe, B. L. (n.d.). Risk mitigation in Digital Twins. Royal HaskoninDHV Digital. Retrieved August 3, 2022, from https://global.royalhaskoningdhv.com/digital/resources/blogs/risk-mitigation-in-digital-twins

Treasury Board of Canada Secretariat. (2021). Access to Information and Privacy Statistical Report for the 2020 to 2021 Fiscal Year. Retrieved December 12, 202, from https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/statis-

tics-atip/information-privacy-statistical-report-2020-2021.html.

Treasury Board of Canada Secretariat. (n.d.). Algorithmic Impact Assessment—ArriveCAN Proof of Vaccination Recognition—Algorithmic Impact Assessment (AIA)—ArriveCAN Proof of Vaccination Recognition. Government of Canada. Retrieved August 7, 2022, from https://open.canada.ca/data/en/dataset/afc17416-3781-422d-a4a9-cc55e3a053c8/resource/540239d2-3703-4fed-9ac5-e7be84934d67?inner_span=True

Tung, T., Billiard, M. C.-, Thomas, M., & Maitin, S. (2020, October 6). Twin-driven and AI-enabled is the future of product development. Accenture. https://www.accenture.com/us-en/blogs/industry-digitization/twin-driven-and-ai-enabled-is-the-future-of-product-development

Ulmer, S. (2021, February 23). Scientists begin building highly accurate Digital Twin of our planet. ETH Zurich. https://ethz.ch/en/news-and-events/eth-news/news/2021/02/a-highly-accurate-digital-twin-of-our-planet.html

Voas, J., Mell, P., & Piroumian, V. (2021). Considerations for Digital Twin Technology and emerging standards (NIST Internal or Interagency Report (NISTIR) 8356 (Draft)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8356-draft

Walters, A. (2019, September 7). National Digital Twin Programme. University of Cambridge: Centre for Digital Built Britain. https://www.cdbb.cam.ac.uk/what-we-do/national-digital-twin-programme

Wang, B., & Burdon, M. (2021). Automating Trustworthiness in Digital Twins (pp. 345–365). https://doi.org/10.1007/978-981-15-8670-5_14

Winkle, W. V. (2021, March 23). Database consolidation takes flight with Boeing's ramp up to Intel Optane persistent memory. VentureBeat. https://venturebeat.com/2021/03/23/database-consolidation-takes-flight-with-boeings-ramp-up-to-intel-optane-memory/

Wylie, B. (2020, May 13). In Toronto, Google's attempt to privatize government fails—For now. Boston Review. https://bostonreview.net/articles/bianca-wylie-sidewalk-labs-toronto/

“... adopt a human-centric and security-focused approach to digital twins, which places digital rights at the core ...”

Human-Centric Cybersecurity Partnership