



## XVIII LEGISLATURA

**Legge di conversione del DL 14 giugno 2021, n. 82**

**“Disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la cybersicurezza nazionale” (AC 3161)**

### **Introduzione**

**Trend Micro, leader globale di cybersecurity, è impegnata a rendere il mondo un posto più sicuro per lo scambio di informazioni digitali.**

Con oltre 30 anni di esperienza nella security e nel campo della ricerca sulle minacce, Trend Micro protegge centinaia di migliaia di organizzazioni e milioni di individui che utilizzano il cloud, le reti e i più diversi dispositivi, attraverso la sua piattaforma di cybersecurity.

Trend Micro ha sedi principali a Tokyo e in Texas, e sedi regionali e centri di Ricerca e Sviluppo in Asia, Europa e Nord America, per un totale di 7.000 dipendenti in oltre 65 Paesi. Trend Micro opera in Italia dal 1998 ed è presente sul territorio con due sedi, una a Milano e una a Roma.

- Oltre 30 anni di esperienza nella security e nel campo della ricerca sulle minacce, hanno consentito a TM di rendere Istituzioni, aziende e persone cyber resilienti grazie a soluzioni connesse che proteggono i workload cloud, gli endpoint, le email, i dispositivi IIoT (Industrial Internet of Things) e le reti.

**Siamo primi al mondo per quota di mercato nella protezione dei Cloud Workload e dell’Endpoint Security (fonte IDC, 2020) e leader da quasi 20 anni nel Gartner Magic Quadrant dedicato alle piattaforme di protezione Endpoint. Trend Micro è anche il vendor che scopre ogni anno più vulnerabilità. Nel**

2020 ad esempio, ha scoperto il 60,5% delle vulnerabilità di tutto il mondo, con il 77% delle vulnerabilità che aveva un livello di alta gravità.

- **Nostro fiore all'occhiello è Trend Micro Research, una divisione specializzata in Ricerca e Sviluppo e nella lotta al cybercrime**, che ci permette di detenere e usufruire della rete di intelligence sulle minacce più avanzate al mondo.

Proprio dal **report di Trend Micro Research sulle minacce informatiche che hanno colpito nel corso dell'anno passato** è emerso come **l'Italia sia il quinto paese al mondo più colpito da macromalware (primo in Europa)** con 12.953 attacchi ricevuti. Mentre il numero totale di malware intercettati in Italia nel 2020 è di 22.640.386; cinque milioni in più rispetto al 2019.

Questi numeri sono stati rilevati dalla **Trend Micro Smart Protection Network**, la rete intelligente e globale di TM che individua e analizza le minacce e aggiorna costantemente il database online relativo agli incidenti cyber, per bloccare gli attacchi in tempo reale. Grazie a questo processo **la nostra rete è in grado di bloccare una media di 65 miliardi di minacce all'anno.**

- **Nel 2021, inoltre, l'Italia si è confermata nelle prime posizioni della classifica mondiale dei Paesi maggiormente presi di mira dai malware.** A gennaio era il quinto Paese più colpito, a febbraio e marzo il quarto, mentre ad aprile sale sul podio di questa speciale classifica come terza nazione maggiormente afflitta dal fenomeno malware.

- Dobbiamo rilevare come, **benché oggi nel nostro Paese si senta spesso parlare di reti, innovazione e infrastrutture digitali, non si riesca tuttavia a porre la giusta attenzione sulla cybersecurity.** In questo ambito certamente si sono fatti passi avanti in termini di regolamentazioni e direttive sia a livello europeo che nazionale, e questo Decreto Legge ne è prova, ma il problema, che realtà come Trend Micro riscontrano quotidianamente, è una **scarsa consapevolezza dell'importanza che ricopre oggi nel Mondo la sicurezza cibernetica.**

Quest'ultima continua ad essere vista come una commodity o semplicemente un adempimento necessario per rispondere a direttive o certificazioni, il tutto però nella costante **sottovalutazione dei danni che un attacco informatico e la conseguente perdita di dati sensibili o blocco generato alle attività può comportare** anche in termini produttivi, economici e sociali.

- **Ecco perché collaboriamo ormai da anni con diverse Istituzioni nel sostenere lo sviluppo dell'innovazione tecnologica e dell'educazione agli strumenti digitali**, nella convinzione che il nostro impegno possa apportare un contributo concreto alle politiche sociali, educative ed economiche del Paese.

Proprio con queste finalità abbiamo realizzato la **ricerca “Project 2030”** (che abbiamo allegato alla presente memoria). **Il suo obiettivo è quello di anticipare il futuro del crimine informatico e permettere ai governi, imprese e cittadini di prepararsi alle sfide e alle opportunità del prossimo decennio.**

Gli scenari che abbiamo cercato di delineare non intendono rappresentare l'intero progresso nel prossimo decennio, ma sono descrizioni di possibili sviluppi tecnologici a medio termine.

Ci siamo invece concentrati sull'impatto delle minacce informatiche dal punto di vista di un individuo, di un produttore e dell'apparato statale. Gli eventi e sviluppi descritti sono prospettati e ispirati dall'analisi dell'attuale panorama delle minacce, dall'opinione di esperti e di specialisti in campi come la sicurezza dell'informazione, la protezione dei dati, la disciplina normativa, la regolamentazione e le relazioni internazionali, tenendo sempre presente il sempre più rapido sviluppo delle tecnologie emergenti.

- **Guardiamo molto positivamente alle misure di supporto e sostegno al digitale e all'innovazione del sistema produttivo** (soprattutto in relazione al Piano Nazionale di Ripresa e di Resilienza) che questo Governo sembra voler portar avanti: investimenti in cybersecurity, l'implementazione delle reti ad altissima capacità e 5G, l'efficientamento del cloud nazionale e l'interoperabilità delle banche dati della PA, sono tutte misure ben in linea con gli obiettivi di innovazione e digitalizzazione più volte ribaditi in sede europea.
- Ma è d'obbligo a questo punto rilevare come l'aumento dell'utilizzo degli strumenti digitali se da un lato ha rappresentato e continuerà a rappresentare una grande opportunità di sviluppo e di crescita per le aziende e PA, dall'altro comporterà un inevitabile aumento dei rischi legati agli attacchi informatici.

**Sono le aziende e le PA che, in un momento in cui la cybersecurity è finalmente riconosciuta da tutti come fondamentale, devono investire sulla**

**propria sicurezza cibernetica, insistere sulla formazione e potenziare le competenze.**

### **Osservazioni sul Decreto-Legge**

- Il primo punto che ci sentiamo di condividere è quello relativo **all'accentramento in capo ad un unico soggetto (l'Agenzia)**, che avrà personalità giuridica di diritto pubblico e che sarà dotato di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, **della gestione della cybersecurity nazionale**. L'accorpamento in favore di un'unica Agenzia di funzioni oggi separate ed in carico a diversi enti è sicuramente un primo passo di un processo di implementazione della sicurezza cibernetica del paese.
- Difficile non condividere inoltre alcune funzioni specifiche delle quali l'Agenzia si farà carico: dallo **sviluppo delle capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione**, degli attacchi e degli incidenti di sicurezza informatica, all'**innalzamento della sicurezza dei sistemi di Information and communications technology (ICT)** dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, delle PA, degli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (FSD).
- In linea con le nostre aspettative anche la previsione del supporto allo **sviluppo di competenze industriali, tecnologiche e scientifiche in un'ottica di autonomia strategica nazionale** e l'assunzione da parte dell'Agenzia delle funzioni di **interlocutore unico nazionale** per i soggetti pubblici e privati in materia di misure di sicurezza e attività ispettive negli ambiti del perimetro di sicurezza nazionale cibernetica.

Fondamentale però che tutti questi intendimenti non restino dei virtuosi propositi ma che riescano ad essere posti in essere in maniera compiuta e organizzata.

La nostra esperienza nel settore ci impone di segnalare che **la sicurezza cibernetica non vuole frammentazione, ma coordinamento e controllo sotto un'unica regia**, con un punto di raccolta unificato e centralizzato per lo scambio delle informazioni interne ed esterne.

- Dobbiamo a questo punto sottolineare l'urgente necessità che la nuova Agenzia sia nelle condizioni di **investire seriamente nella sicurezza cibernetica e nell'attività di intelligence relativa alle minacce**. Conoscere, decrittare e anticipare la minaccia è la condizione essenziale e necessaria per scongiurare il rischio di essere colpiti.

È fondamentale quindi che venga sviluppato **un piano di investimenti e strategie per la cybersecurity che coinvolga l'intero sistema, pubblico e privato, economico e sociale**.

Sarebbe opportuno, subito dopo, cominciare da un **insieme chiaro e definito di procedure e norme a cui gli enti pubblici e le aziende che trattano dati sensibili dovranno conformarsi per proteggere i propri sistemi**.

- Siamo convinti che si dovrebbe prevedere un **maggiore coinvolgimento della parte apicale delle aziende pubbliche e di quelle private, per stimolarne la collaborazione e configurare un'architettura di sistema quanto più possibile pronta a prevenire, a difendersi e a rispondere ai cyber attacchi**: l'istituzione dell'Agenzia per la Cybersicurezza nazionale potrebbe rappresentare in tal senso una grande un'occasione.

In questa direzione è necessario assicurare che le **attività di reazione e stabilizzazione siano condivise con linee guida standard** che, però, tengano conto di analisi del rischio basate su indicatori semplici da applicare ad enti della Pubblica Amministrazione centrale e locale.

Fondamentale inoltre **l'implementazione di un sistema di interscambio di informazioni tra pubblico e privato in *real-time***, in modo da risolvere o addirittura prevenire incidenti informatici.

- **La collaborazione con il settore privato dovrà convergere non solo sui sistemi di prevenzione e risposta, ma anche per la parte riguardante la formazione e l'educazione al digitale**: le aziende del settore infatti hanno la possibilità di segnalare le *best practices* e di informare l'Agenzia sugli incidenti che accadono giornalmente nel mondo *small/medium business*, oggi non compreso nell'ambito del perimetro di sicurezza nazionale, ma con il quale interagisce giornalmente.

Necessario dunque investire sulle **competenze digitali** in tutti i settori della società e per una formazione riqualificante per i dipendenti pubblici e privati.

- Riteniamo, inoltre, che ogni politica pubblica che andrà nella direzione di mettere la cybersecurity al centro del sistema non potrà mai prescindere da un **cambio di paradigma a livello centrale e da una modifica dell'organizzazione e dei processi tecnologici oggi esistenti nella PA e nelle aziende.**

Con la diffusione delle nuove tecnologie, infatti, si moltiplicano i relativi rischi legati agli attacchi informatici e alla gestione di tutti quei dati sensibili che rilasciamo sulla rete.

In generale, e gli ultimi casi di attacchi a imprese molto note sul mercato e a PA lo dimostrano, appare ormai evidente come la sicurezza cibernetica debba diventare non solo uno dei pilastri dell'attività di un'organizzazione pubblica e privata ma anche il **presupposto necessario di un'architettura nazionale di rete agile, evoluta e flessibile per il futuro.**

**La cyber resilienza dovrà diventare l'elemento fondante e abilitante del nostro presente e futuro tecnologico:** tutti i servizi, le piattaforme, le applicazioni digitali non potranno non rispondere a determinati standard di sicurezza.

Sarà quindi necessario lasciarsi alle spalle il vecchio approccio settoriale e adottare un approccio sistemico prevedendo misure di cybersecurity che guardino l'insieme delle strutture, integrate e comunicanti tra le missioni e le linee progettuali relative alla digitalizzazione nel nostro Paese.

## Conclusioni

- La pandemia ci ha mostrato come il concetto di prevenzione del rischio di attacchi cyber sia assolutamente mutato, **passando dal semplice presidio del perimetro aziendale alla necessità di monitorare un orizzonte sempre più esteso, fatto di reti pubbliche, private e domestiche.**

I recenti casi di cronaca con attacchi massivi ad aziende molto famose e PA ribadiscono l'importanza di investire su un **nuovo concetto di sicurezza cibernetica** che permetterà un cambio di paradigma nella prevenzione dei rischi legati agli attacchi informatici.

- Volendo andare anche oltre i contenuti del Decreto Legge, dobbiamo osservare che per rafforzare compiutamente la filiera della cybersecurity sarebbe prioritario prevedere l'obbligo per imprese e PA di adottare **prodotti, strumenti e tecnologie "hack**

**proof**”, e di dotarsi della figura di **Chief Information Security Officer (CISO)** e, per determinati contesti, di certificazioni «accountable» (es. ISO 27001).

- Sempre a questo proposito si potrebbe contemplare lo **stanziamento di risorse per l’ammodernamento informatico dei sistemi IT delle PA** per porre rimedio all’obsolescenza dei sistemi attuali che utilizzano tecnologia facilmente aggredibile dall’esterno.

Nel settore privato, invece, è imprescindibile a questo fine la previsione dell’**aumento dell’agevolazione fiscale del credito d’imposta sull’acquisto di software, sistemi, piattaforme e applicazioni per la protezione di reti, dati, programmi, macchine e impianti da attacchi, danni e accessi non autorizzati.**



# PROJECT 2030

## Scenarios for the Future of Cybersecurity

Dr Victoria Baines & Rik Ferguson

Endorsed by:



Every year we all see many reports aggregating the results of surveys - and quite a few that seek to extrapolate the results into the future - but rarely do we see a report that is as thought-provoking and insightful as "Project 2030 - Scenarios for the Future of Cybersecurity."

The report's authors, Victoria and Rik, create a picture of what life for real people could look like only nine short years from now, and look at the cybersecurity picture through the lens of the impact of technology from the perspectives of people, business and countries.

Many reports on cybersecurity are, to paraphrase Winston Churchill, a sum of all our fears, or a dry recitation of facts and figures. Project 2030 is anything but.

Of course, the future that Project 2030 posits will not be realised exactly as we see it here - but we can see in its pages elements which are almost certain to be realised: from the impact of 'deepfakes' on increasingly connected people, to dramatic changes in production due to automation, and supply chain security issues.

What is of overriding clarity is that cybersecurity issues will become more and more important not just as policy objects, but to the general public, the more we are connected to one another through technology. We all know this at some level, but what this report does very persuasively, is show us why the cybersecurity problems of today, and how we approach them, are integral to the health and well-being of us all tomorrow.

The opportunities that technology has to offer us today are only a small portion of what we will see in a few short years. This report should provoke a great deal of thinking - and it should also provoke action. ICC United Kingdom is increasingly active in international cybersecurity policy precisely because it is the key to a shared future of opportunity that minimises risks and promotes healthy outcomes.

ICC United Kingdom are proud to endorse and recommend "Project 2030 - Scenarios for the Future of Cybersecurity."

**Chris Southworth,**  
Secretary-General, ICC United Kingdom



**UNITED KINGDOM**  
INTERNATIONAL  
CHAMBER OF COMMERCE

The world business organization

# Contents

---

**04**

Security challenges and the nature of threats

**05**

The View from 2020

**07**

Scenario Narratives for 2030

**07**

a. Citizen – Resila

**11**

b. Business – KoRLo Industries

**15**

c. Government – New San Joban

**19**

Cyber Threats

**23**

Implications for Cybersecurity Stakeholders

**28**

Beyond 2030

**29**

Appendices

**29**

Scenario Method

**30**

Timeline Validation

**31**

Survey Questions

**33**

Survey Responses

# About Project 2030

“Human beings are really bad when it comes to innovation. We persistently overrate the short term impact of technology change, and underrate the long term impact of technology change.”

Live poll participant, December 2020

Project 2030 is a Trend Micro research initiative. Its aim is to anticipate the future of cybercrime, and to enable governments, businesses and citizens to prepare themselves for the challenges and opportunities of the coming decade.

The scenarios that we outline are not intended to represent the entirety of progress over the next decade. They are descriptions of possible medium-term technological developments, with a focus on the impact of cyber threats from the perspectives of an individual, a manufacturer and the apparatus of state. The events and developments described are designed to be plausible in some parts of the world, as opposed to inevitable in all. They are informed and inspired by analysis of the current threat landscape, the expert opinion of specialists in fields including information security, data protection, law enforcement and international relations, and extensive horizon scanning of emerging technologies.

The authors would like to thank Sara Hook of Pulse Conferences for assistance in conducting the live poll of technology timelines, Neil Walsh for assistance in soliciting survey responses, and Damien Batchelor for specialist advice on the future of nanomedicine.

# The View from 2020

Synthesis of threat reporting from international organisations and leading cybersecurity providers facilitated the identification of a baseline of cybercriminal threats in 2020. Threats, enablers, and other features of the cybersecurity ecosystem identified by international organisations were as follows:

Threats & Vectors		
Adversarial AI	DDoS	Malicious USB mailing
Botnets	Doxxing/ information leakage	Physical manipulation/damage/loss
Business email compromise	High profile data loss	Ransomware (targeted, high value, third party attacks)
Business process compromise	Influence operations/disinformation	Remote access trojans (RAT)
Credential stuffing	Insider threat	SIM swapping
Crime as a service	IoT compromise or DoS/ Edge attacks	SMiShing
Cryptojacking	Logical ATM/PoS attacks	Phishing (themed/spear-/whaling)
Cyberespionage	Malicious apps	SQL injection
Data stealing trojans (Emotet)	Malicious domains	
Web exploits	Supply chain & third party compromise	
Enablers & Targets		
Cloud/virtualisation	Mobile	Misuse of legitimate business structures/tools
Criminal infrastructure (bullet-proof hosting)	New ways for criminals to hide	Social Media
Criminal opportunism	Privacy-enhancing wallets	Deepfakes
Darkweb evolution/ regeneration	Social Engineering	
Online financial services	Unpatched/discontinued/ legacy applications	
Ecosystem		
Automated detection	Criminal opportunism	New threat actors

Fig.1 Common features of 2020 cyber threat reporting from select international organisations<sup>1</sup>

<sup>1</sup>Based on manual review of Europol's Internet Organised Crime Threat Assessment 2020, ENISA's Threat Landscape 2020 (Year in Review, Threat Intelligence, and Emerging Trends reports), and Interpol's COVID-19 Cybercrime Analysis Report.

Common features of cybersecurity industry threat predictions in 2020 were grouped as follows:

Threats & Vectors		
API attacks	Advanced Persistent Threat (APT)	IoT-related attacks
Ransomware/double extortion		
Enablers & Targets		
5G & Telecoms	Cloud & Edge	COVID-19 exploitation
Automation & Artificial Intelligence	Consequences of teleworking/ schooling	Deepfakes
Legacy vulnerabilities		
Ecosystems		
Cybercrime gang cooperation	Security automation	User privacy
Regulatory & enforcement activity	Shorter patch windows	

Fig.2 Common features of 2020 threat predictions from select cybersecurity providers<sup>2</sup>

The aim of the rapid review was to ensure a threat baseline for the scenarios that was as complete as possible. Therefore, no attempt was made to compare the findings of the international organisations with those of the cybersecurity industry, or to reduce the respective features to comparable categories. Rather, all identified threats and vectors, enablers and targets, and features of the current cyber threat ecosystem were taken into consideration when building the scenarios. As a result, there is considerable overlap between items listed in Fig.1 and those in Fig.2. For example, nation state or state-sponsored Advanced Persistent Threat (APT) as outlined by industry in Fig.2 maps to cyberespionage as described by international organisations in Fig.1: indeed, it is the same threat conveyed in different terminology.

The COVID-19 pandemic inevitably looms large in cyber threat reporting for 2020. Exploitation of the pandemic, manifest in themed phishing, SMiShing and cyber-enabled frauds, but also in the nation state arena with reported attempts to compromise vaccine research, speaks to a long-standing bent of cybercriminal opportunism. Rapid virtualisation of businesses and education was likewise deemed to be a key situational vulnerability and attack vector by industry and international organisations alike. The scenarios in this document were drafted against the backdrop of accelerated mainstream adoption of certain technologies: current nuisance activities such as zoombombing served as signals for criminal misuse of emerging technologies en route to 2030.

Industry reporting in particular points to a greater awareness of cyber-physical threats than ever before. Once considered largely in terms of threats to critical infrastructure, hacks of things (IoT) and of systems

---

<sup>2</sup> Based on manual review of threat reporting from BeyondTrust, Checkpoint, FireEye, Fortinet, Kaspersky, LogRhythm, Symantec, Trend Micro and WatchGuard.

on which human security depends are featured in the 2020 cyber threat predictions. To some extent this is due to a more consistent focus on automotive cybersecurity. Highly publicised ransomware attacks on hospitals battling the pandemic have also served as signal crimes for the future development of cyber threats resulting in physical injury. The announcement of a homicide investigation into the death of a German citizen following a ransomware attack is perhaps the most notable example in 2020.



**“ Industry reporting in particular points to a greater awareness of cyber-physical threats than ever before. ”**

Prominent in reporting from both industry and international organisations was a recognition of the blurring between state and non-state cyber threat actors, whether in the form of influence operations and disinformation, cyberespionage, APT, or extortion (ransomware). A related concern, understandably discussed more explicitly in the industry reports, is the extent to which cybersecurity has become a geostrategic issue, particularly with respect to supply chain and procurement. In addition to the cybersecurity industry predictions, international organisations also included in their reporting a certain amount of future-oriented threat considerations: for example, the use of deepfakes and 5G as threat vectors and enablers was mentioned, although not yet mainstream in 2020.

As was the case for the synthesis of threat reporting for Project 2020, this readiness to look ahead provides a helpful springboard to imagining a mid-term future in which the presumed constant of criminal misuse plays out against a backdrop of continuous technological development.

# Scenario Narratives for 2030

## a. Citizen - Resila

Resila has lived in New San Joban all her life. Her parents met while studying at the university in the last century. Both her children were born here. As a citizen of one of the most technologically advanced cities in the world, Resila knows that there are many reasons to be thankful to technology.

Resila always hated shopping. When she was a child, her mother would take her to the supermarket every Saturday. Every year, she would be dragged around town and made to try on new clothes and shoes for school. Resila's children no longer have to do any of that. Sensors in the childrens' clothes take continuous tailored measurements of their dimensions, to ensure their replacements are just the right size and delivered at the correct time.

Wearable sensors also identify the family's nutritional needs, including vitamin and other deficiencies. Resila has opted in to a service that automatically orders supplements and adjusts the content of her shopping basket, increasing fibre and reducing fat and carb content as the need arises. The online supermarket shelves display only the items permitted or beneficial. Other customers whose medical data cautions against certain products (alcohol or sugars, for example) are able to request that they be locked out of that section of the store. The groceries and supplies they regularly use are automatically reordered and delivered by drone.

A premium service links this nutritional data with the health records held by Resila's doctor, her gym membership and her sleep patterns, and even her gut health by means of a connected toilet bowl. Resila's contact lenses routinely test her lacrimal fluids for a number of common acute and chronic health conditions, including cancers, stroke risk, and diabetes. Anomalies trigger appointments for further investigation, consultation and treatment. The more squeamish members of society opt for skin-like patches instead. These are used to monitor and report changes in sweat composition, also to administer prescribed drugs continuously. Having been commercialised for over a decade, DNA profiling is also now contributing directly to preventative healthcare.

3D printing has dispensed with the need for meat production: now Resila just prints what she needs at home. At first she wasn't convinced that the idea would take off. But growing citizen concern for healthy living and the environment, rising haulage costs, and the phasing out of fossil fuels have provided fertile ground for trendy restaurants to monetise their recipes, incorporate dietary supplements, and link up with the raw material producers. Resila is pleased to be doing her bit for the environment, but makes sure to double check the recipe before hitting the print button, and keeps an eye out for public safety announcements. Last year, hackers altered some of the ingredient lists on the most popular subscription service, and a bunch of people got food poisoning.

Healthcare has come on in leaps and bounds in the last decade. Wearables became more sophisticated, then data and drug discovery became more powerful. Resila's father takes anticoagulant medication, as do a lot of people his age. He used to have to go to the hospital for regular blood thickness tests. The doctor would then adjust his dosage accordingly, contact him by phone, and then he would have to remember which pills to take. Now, his wearable monitor takes and analyses his blood, his prescription is automatically updated and instructions are sent to his home 3D printer. When he biometrically authenticates to the printer, his entire drug regimen is analysed and polypills are dispensed in the required dosages, minimising the total number of pills to be taken. In some countries, human validation has been removed entirely from this process. New San Joban, however, has enacted legislation mandating human review of drug dispensation. Of course, mistakes are still made. Resila's father has been offered one of the new nanorobotic treatments, and while Resila thinks it could be a safe option, he prefers to have some control over the drugs in his body.

Battery storage has become considerably cheaper and more efficient in recent years. Each new home in New San Joban incorporates compact thermoelectric generators within its construction material, and features solar capture and a home storage battery, all of which are connected to the city grid. The grid runs as a community enterprise, administered by the local authority. Citizens like Resila contribute through their local taxes. In return, power generated stays within the city limits.

The connected home has reached maturity. Just ten years ago, Resila had to use voice commands and manually configure each device to the central hub. Now, all the devices talk to each other, automatically adjusting to environmental changes, occupation and calendar events, and she only needs to update them via the controller when she wants to change a setting. The downside occurs when one of the devices, or increasingly, the information they gather through local and cloud APIs, is compromised – it was so embarrassing last year when she had invited friends round for dinner and she couldn't let them into the house or turn the lights on.

Resila's son Kojo has been pestering her for a neural implant, but she's not so sure. His attention span is quite short to begin with, and kids are already bombarded with too many distractions via their lenses. But Kojo has a friend whose grandma has an implant. It mitigates the symptoms of her Parkinsons disease, monitors vitals and other bio signs, uses GPS and an accelerometer to identify when and where she may have had a fall, registers the force and direction of trauma and summons emergency services if necessary. It also enables her to control her synthetic arm and anything else with which she chooses to connect – and it is the coolest thing Kojo has ever seen. Resila has tried to explain that medical necessity is different than just wanting one for fun. But Kojo is a committed gamer. Now that physical sensation has been enabled, feeling 'really there' has become a big part of young people's lives in particular. Being physically present in gamescapes requires ever faster response rates. Friends of his with implants are now playing at the speed of thought, and he is at risk of losing his edge.

When they're studying, the kids are only supposed to have the school layer active on their lenses. But no matter how much Resila tries to enforce the parental controls, Kojo always seems to get around them. Mixing the layers mixes the behavioural data captured by the sensors. So, when Kojo starts drifting off in class, scammers target him with ads for stimulants and mods that make him look like he's paying attention. Even when he has only the school layer on, people have worked out how to hack into the system and show him things he doesn't want to see. Kojo's school gives lessons on respectful behaviour and personal space. But inevitably there are kids who break the rules and hurt others, and people of all ages are finding it challenging to have to question what they see with their own eyes.

Instant access to the world's knowledge has obviated the need to learn anything. Education is now focused on processing, rather than acquiring, knowledge. As a result, people increasingly know less objectively. What Kojo and Resila see before their eyes is determined by algorithms. Algorithmic Optimisation has become a key technology in the battle literally for hearts and minds. Search results are now the subjective truth: manipulating these is a target for those looking to spread disinformation and propaganda. As more people have opted for implants, this has raised the possibility of changing people's belief systems more efficiently and more directly, for good or ill. Governments around the world have now contributed funding to a United Nations project to establish an objectively factual record of current and historical events. Perhaps inevitably, it has proved difficult to get some countries to agree on the facts of a surprisingly large number of issues.

Resila has already noticed the difference in her own behaviour. When she was looking at her phone or laptop screen, she could detach herself from sensational posts and news stories. She could step back and take a minute out to fact check them. Now, hyper-personalised headlines are delivered directly into her field of vision. Constrained by the lenses' character limits, mainstream news is now essentially clickbait, with added emotional engagement and the psychological impact of not being able to look away. Scammers and influence operators have been able to capitalise on the opportunities of a more captive audience.

The working world has changed so much since Resila started her first job twenty years ago. New working practices introduced during the Great Pandemic showed that many people could work perfectly well from home. When web conferencing was found to be too dry and impersonal, virtual and augmented reality stepped in to provide companies with the immersive and realistic remote workspaces employees were lacking, and real telepresence. With 3D visual overlays, gesture capture and behavioural productivity metrics now standard, Resila can now work from anywhere. Her employer, KoRLo Industries, now operates just one physical office space globally, and that is in a different country.

For local trips, Resila cycles or takes a taxi pod when she feels lazy. Her car remains in the garage since she decided not to renew the tax and insurance when the kids were old enough to cycle themselves or use the new Personal Rapid Transit pods. Older people and those in the countryside still have cars. Since the imposition of a prohibitive fossil fuel duty, the majority of these are electric. As of this year, no new petrol, diesel or hybrid vehicles are being sold and fuel stations are becoming scarce.

It felt pretty strange the first time she got in a driverless taxi pod. But living on a smart road made it a no-brainer, and she got used to it pretty quickly. Her parents have taken more convincing, and she still gets the occasional voice call from her Dad when he has forgotten his travel chip, or ended up on the wrong side of town. Cars are no longer allowed in the city centre, where dedicated lanes for driverless vehicles, ebikes, scooters and pedal bikes now dominate.

Downtown New San Joban is very different to how it was when Resila was a child. Then, it was hectic, full of office workers and noise in the week, almost empty at weekends. Increased teleworking has led to companies giving up expensive office space. Faced with downtown desertion and potential deprivation, so-called “bright-flight,” the city innovated at the expense of the out of town shopping malls. Rents were slashed for residential, recreational, social and creative uses, and there is now a vibrant leisure hub. They’re calling it ‘recentralization.’ And, as the city centres are repopulated, the suburban sprawl is shrinking, leaving behind ghost districts and ghost suburbs.

Resila likes to bring the kids into town to play tennis and have coffee. In contrast to cities with younger populations, there is still some retail space, because some older people feel more comfortable interacting with a person and seeing physical goods before buying. A couple of years ago, Resila was elected to the city council. She is fiercely proud of her home town’s ability to adapt in a changing world.

People’s digital versions of themselves have become so extensive as to require dedicated management. Resila uses a tool that broadcasts her privacy preferences to every service that requires her data. The tool grants permissions that are contextually sensitive, the data is homomorphically encrypted, and only Resila has access to it. When a new service needs to use her data, it is granted only access to the information required based on set rules and in accordance with legal restrictions.

At the same time, humans have now volunteered so much of their lives through self-generated content that archives for individuals have not only become necessary; they have resulted in digital selves that outlive the physical death of a person. What was once a collection of memories on social media is now a seemingly living thing. By continuing to interact in social spaces, they provide comfort to the relatives they have left behind. While the first generation of these ‘infini-mes’ tended to repeat a restricted set of interactions based on data they had been fed in the physical human’s lifetime, the latest versions are self-learning, and able to engage in new experiences based on physical humans in their closest peer and interest groups. Increasingly, these digital humans have agency, particularly as the physical and digital worlds combine. They engage in inappropriate behaviour, and sometimes commit crimes like hate speech. Government authorities are now considering whether they are culpable, and what appropriate enforcement measures might be for their illegal activities. Grieving families, meanwhile, have sought the help of human rights lawyers to prevent their loved ones being switched off, or in some cases to enforce that they are.

## b. Business - KoRLo Industries

Konsolidated Rubber and Logistics (KoRLo) Industries is a heavy manufacturer with a two hundred year heritage. Having diversified from natural to synthetic rubber products in the second half of the last century, KoRLo became a global leader in tyre, technical clothing and cable manufacturing, to name but a few. Expansion into medical glove production and wearables during the Great Pandemic brought the company further into healthcare supply, while its work on synthesising self-healing polymers has seen its products used in submarine communications cables and a proliferation of low earth orbit satellites. These products alone designate KoRLo a critical infrastructure supplier.

An increasing number of KoRLo's products contain sensors that are dual purpose. Once in their end use operating environments, they analyse and report on - for example - wear on the tread of a boot or tyre, alerting the owner to the need for repair or replacement. In space and on the sea bed, they predict impending failures in polymer seals and cabling insulation. They give accurate diagnostics of catastrophic failures in their operating environments, and contribute to meteorological reports. As part of its corporate social responsibility efforts, the company also sponsors and provides components for a leading ocean clean up initiative, and is leading a research program to look at how its cable insulation might attract microplastics to clean up the seabed.

Where the polymer is not self-healing, or where the self-healing is compromised for some reason, infrastructure owners can deploy fully autonomous undersea repair vehicles. These patrol the length of cables continuously, and can also gather data about the health of the ocean floor. Recycled granular plastic now makes up the majority of KoRLo's raw material: the company has recently reached the landmark target of 80% plastic recycling as stipulated in international agreements. This model has also enabled KoRLo to move its production closer to sea and space ports, further reducing freight costs and environmental impact. The reuse of old 'brown field' industrial facilities is a key part of the company's circular strategy.

Monitoring of the supply chain and production line is now entirely digital. Advances in AI and analytics mean that in the majority of instances physical items and data are self-routing and self-healing. In addition to predictive and preventative maintenance, integration of KoRLo's customer service, procurement and operations means that every customer order triggers an automatic stock check, reordering of precursor chemicals and other components if necessary, and despatching instructions to the company's semi-autonomous cargo fleet and - increasingly - the freight hyperloop. The result is greater efficiency and speed, shorter downtime, and lower resource costs. These developments in automation, self-remediation and autonomous logistics have resulted in an increased focus on security technologies that prioritise system, data and process over confidentiality and availability. In many uses cases now it is preferable to shut a process down completely rather than allow it to continue running in a corrupted or degraded condition.

KoRLo does not own or operate any of its IT infrastructure. All supervision, maintenance and operation takes place in the cloud; every factory is smart and connected by platforms supplied as a service. Any proposed new production or changes to existing operations are tested in the company's digital twin before being rolled out in the live environment. Because KoRLo makes things that are programmed to change shape, its DevOps have taken on an industrial, physical quality, merging with hardware and chemical design. The company's personnel refer to this hybrid process as DesOps; in some other parts of the world, the term MakeOps has become popular. The challenges in the adoption of this totally outsourced infrastructure have been considerable. KoRLo now has to identify and manage an exponential growth in user profiles, rather than manage a simple user population: each device brings its own attack surface and must also be continuously identified and assessed. Their proprietary and PII data is stored in and accessed from more systems than ever before and through multiple software interfaces.

KoRLo's human employees are involved in three core activities: checking automated work, investigating and responding to the more serious anomalies, and setting business strategy. Resila works on the last of these. As head of the Design Strategy team, she was instrumental in the company's acquisition of 4D printing capability. This has proved decisive for KoRLo's shift to production of flat-packed items suitable for space transit that can change shape on GPS stimulus. Additive manufacturing has also taken the company further into healthcare, specifically bioengineering. Their recent partnership with Medist8 to provide self-folding polymer stents was promising; the next stage of development brings a new departure into programmable printed tissue.

Resila's role has changed considerably. When she first started out twenty years ago, she used computers to design dumb products. Her biggest security concern was around theft of designs by competitors and nation states. Then came IoT and the incorporation of actuators and sensors into so many product designs. While some of KoRLo's markets still have different standards, high profile attacks and lawsuits have set the de facto international threshold and risk appetite. A few years ago, alleged nation-state aligned compromise of an operating system for home appliances caused mass panic when home batteries started overheating. Some exploded or caught fire. Customers affected are now suing the manufacturer for emotional and physical injury.

Intellectual property theft remains a concern, of course. In addition to simple exfiltration, manufacturers like KoRLo are having to defend against data-poisoning attacks. There is a vibrant underground market for stolen designs. Criminals have also developed the means to alter the composition of designs so that the end products do not function as intended: open source templates have proved particularly vulnerable to poisoning. At its least harmful, the impact entails downtime and the costs attached to suboptimal functioning. In the context of the company's sensitive medical and military contracts, the stakes are somewhat higher. Malicious data and process manipulation could lead to physical harm.

And with so much of the design process now automated, poisoning of the machine learning algorithms themselves, or the data pools from which the tools learn, can also lead to unpredictable outcomes, as well as flaws and safety issues in end products. While some criminals have the demonstrated capacity to do this, in many cases the threat is enough to generate a profit. Extortion remains a common tactic and, as ransomware proved back in the day, people, businesses and their insurers are often prepared to pay up. Denial of Service and other forms of malicious disruption and interference can occur at the design stage, in production, shipping and during end use – all of which KoRLo is liable for to some degree.

For several years now, there has been considerable interest in the possibility of eavesdropping on people using the company's consumer oriented products. Many more sensors now mean many more data points by which to triangulate and extrapolate an individual's behaviour and movements. A research study using data from sensors in KoRLo's hiking boots suggested a link between levels of activity indicated by tread wear and anxiety. Privacy advocates and mental health charities are now concerned that the company is aggregating this data with information reported by its medical wearables, and that it is open to access by law enforcement and other government authorities. Rumours that the company is also considering ways to monetise the data by offering telemetry to healthcare providers and the insurance industry are gaining ground.

This is all fuel to the flames for the conspiracy theorists, who have inevitably moved on from vaccines and phone masts to what they see as surveillance tech within the body – nanomedicine, bioengineering, and connected implants. KoRLo has been implicated in this and, however inaccurate it may be, regularly receives threats of violence. The company's public relations department now has a team dedicated to fact checking and conspiracy rebuttal. A shooting at a competitor's facility a couple of years' ago, and the frequency with which KoRLo identifies attempts at automated and massively distributed Denial of Service attacks on its own systems, suggests that these are not empty threats. Botnets have evolved: using compromised IoT, it is now possible to launch internal DoS attacks using the company's own massively connected devices.

For this and other reasons, enhanced vetting of employees has become increasingly important. Insider threats have always been a problem, and while KoRLo makes extensive use of sophisticated access controls and identity management tools, spotting unauthorised access, interference and exfiltration is an increasingly complex task. Many of the company's staff hardly ever set foot in its offices or factories. The digital noise generated by the millions of devices active in or produced by its operations is considerable. None of these devices exist on corporate infrastructure, but rely on 5G connectivity and processing is carried out in distributed edge computing in the public cloud.

The frequency, volume and speed of automated attacks has required that KoRLo invest heavily in automated and intelligent defence. What used to be called Business Email Compromise no longer requires human error. In a fully automated supply chain, invoices are paid without human authorisation.

In its place, Business Process Compromise has evolved. KoRLo and other large corporations now use distributed ledger (blockchain) technology to prevent and identify process anomalies. Tier 1 Security Operations tasks are now fully automated: humans now deal only with cases triaged and escalated by artificial intelligence.

The move to augmented and immersive interfaces for the human employees has also put a premium on automated defence. As soon as the lenses and smart virtual rooms were deployed, phishing attempts became more successful. Eventually, companies around the world realised that it was harder for employees to dismiss, and more likely that they would fall for, scams in their immediate line of sight, or in spaces in which they were immersed. They were also more upset by adverse experiences at work. Zoombombing, a phenomenon originally named after an early video-conferencing technology that gained traction during the Great Pandemic, has evolved as the environment has become more immersive. This has generated increased enthusiasm among the employees for security awareness programmes. Despite the growing technical complexity of security incidents, the human line of defence has not disappeared entirely. The challenge now is how to train employees to identify suspicious or inauthentic activity and offer them contextually appropriate tools to report and dismiss it, in an environment where they routinely interact with realistic, digital versions of their colleagues, driven by generative adversarial networks (GAN).

KoRLo's non-human workers, meanwhile, are as productive as ever. The company's profits depend on it. As a result, it is part of the security team's brief to minimise the risk of the 'Rogue Robot' scenario, and to ensure that their operating environment is constantly tuned to minimise negative experiential input. But with so many end points and so many APIs on so many different networks, the race is on.

### c. Government - New San Joban

The city of New San Joban (NSJ) is at the forefront of tech adoption. A number of leading tech companies have their headquarters in or near the municipality, and it is often used as a testing ground for emerging technologies. The residents of NSJ are also some of the most privacy minded in the world. A few years ago, the national government took the unusual step of holding a referendum on whether to have a single digital identity for all its citizens. NSJ not only reported the highest voter turnout; its citizens also returned a resounding 73% against aggregating their travel, health, tax, employment and education data. The national result was a close run thing, with 52% against and 48% in favour.

While the referendum was not legally binding, the result has been accepted as the will of the people - for now. The national government argues that a single digital identity for all will bring greater efficiency and security. Privacy advocates are understandably concerned about the potential for ubiquitous surveillance, and for unfair treatment as a result of cross-profiling.

In the neighbouring state of East San Joban, the authoritarian regime has banned 'undesirable' people from teaching for fear that they will corrupt the young. People who pay their taxes late are prohibited from using public healthcare.

In New San Joban, the city council has sought greater data aggregation to incentivize good behaviour in the circular economy. Households whose smart bins register that they recycle as instructed already receive discounted public transportation. Pedal cyclists and e-bikers identified as 'responsible and respectful' get discounts on food and drink in the social zones downtown.

Security experts have observed that while combining the different data sets may be useful to those tracking terrorists and criminals, it would also be of great value to hackers and influence operators. Two responses of note have emerged. An increasing number of citizens around the world are using security tools to ensure that their data sets are kept separate, and many are resisting digital data collection altogether. These "Splitters," as they have come to be known, are often aligned with environmental activists and off-gridders. Because NSJ is a smart city, it's effectively impossible to live there off-grid, so there is a growing alternative community in a rural area about 20km outside the city limits. At the same time, some supporters of the benefits of a single digital identity are advocating stronger legislation and greater transparency in relation to government surveillance and differential privacy. The latter has been gaining ground for a number of years now, enabling the benefits of big data analysis for e.g. healthcare provision, while reducing – but not entirely eliminating – the exposure of real identities.

Single use plastics are entirely banned in NSJ, and plastic in all its forms is being phased out. Because fossil fuel derivatives are also outlawed, local manufacturers (KoRLo's competitors among them) are in the throes of shifting their production to bioplastics. One company, Compfabrik, sponsors the local high temperature industrial composting facility where waste bioplastic is used to generate heat and power for the city.

A decade ago, trade sanctions on foreign communications infrastructure components delayed the deployment of 5G technology in many countries. The national government resurrected homegrown telecoms companies' manufacturing, and committed to a programme researching materials and equipment required to launch 6G. The country is set to become a leading supplier of 6G technology and components to allied nations. But there is now greater technological disparity between sovereign states than ever before.

Large scale deployment of 5G in New San Joban has been achieved through component supply from companies in 'friendly' countries. It has enabled some of the key innovations in this smart city, including connectivity that appears seamless to individual citizens, continuous augmented vision and projection away from home, and one of the most sophisticated transportation networks in the world.

Proximity to a world leader in driverless vehicle technology encouraged the city council to designate special lanes for semi-autonomous taxipods in geofenced areas of new housing. Downtown is now petrol-free. The council stopped short of full integration as there are still many thousands of petrol and hybrid vehicles registered in the wider city. A massive increase in fuel duty early this year is already changing consumer behaviour and funding council innovation.

NSJ is an entirely cashless society. Debit and credit cards are still used by the elderly, but are otherwise very much in decline. A digital currency, tied to the national fiat currency, is widely used and endowed with a range of biometric features including payment confirmed by facial recognition. It does not, however, offer anonymity, and is therefore shunned by the privacy- and criminally-minded alike. As cash became less and less popular, criminals who continued to use it in the open were very quickly identified; now they ship it to other parts of the world where it can be more easily exchanged for crypto.

As part of her voluntary security role for the council, Resila works with the police and national cybersecurity service. At a national level, law enforcement and intelligence agencies are preoccupied with influence operations by foreign state actors, and particularly their interference in the democratic process. While solutions have been developed to help identify faked or altered audio and video of political figures, widespread use of synthesised audio and video in the entertainment industry and by legitimate political campaigns complicates their effective use. Citizens have become desensitised to footage generated by AI, which is now so accurate and so lifelike that citizens are unable to tell the difference between synthetic and authentic content. At the same time, delivery in citizens' line of vision makes this material harder to ignore, more credible, and more emotionally immediate. Those who once doubted the real impact of influence operations now face its more effective descendant. Disinformation has evolved into fully-fledged immersive conversations with artificially generated avatars, capable of changing citizens' minds or even corporate policy.

Technonationalism has not been confined to communications infrastructure. Supply chains have been under close scrutiny in the public and private sectors for a number of years, following high profile attacks involving compromised digital components. While larger businesses have, to some extent, absorbed the added costs of more selective procurement, local government contracts have taken longer to restructure. Perhaps more critically, government customers like the city council of NSJ have not enjoyed the same budgetary luxury as their private sector counterparts. As someone with experience in supply chain security, Resila has been asked to provide oversight for the council. She has noticed that when it comes to security, it's not just the supply chain that's affected by budgetary restrictions. Financial constraints also dictate the human and technical resources available for security. And in a smart city like NSJ, failure to secure can result in physical destruction and bodily harm, particularly when next-gen ransomware and data poisoning attacks result in denial of or interference in smart city management, and expose APIs for transportation, healthcare, education, taxes, logistics and other services.

In the age of the Massive Internet of Things (MIoT) and 5G, everything is connected via a SIM. The interconnection of a massive number of devices and sensors has spawned new types of attacks, and some new vectors for old attacks. Law enforcement saw the smart city botnet coming, but not the potential for IoT compromise to be monetised by means of toll fraud. A few months ago, the council discovered that some of its street lights had been calling premium rate phone numbers. An international police investigation has found that many millions of vehicles and home appliances have also been compromised, and that the owners of the phone lines are cashing in.

The newly established International Public Prosecutor's Office is looking to bring charges, but the country in which the criminals appear to be located is not a party to this organisation, and is allegedly refusing to comply with the prosecution.

International commitments against criminal misuse of IT have made multilateral action against some non-state bad actors possible, and their trials have received considerable public attention. But there is tacit acceptance that the most dangerous criminals are still state-sponsored. Likewise, agreements on states' appropriate use of offensive cyber operations have not eliminated attacks by groups whose state affiliation is increasingly difficult to determine. The need of national governments to be seen to condemn illicit activities has accelerated the evolution of tools that make timely attribution of cyber attacks even more challenging. Multi-sector initiatives to establish norms and principles for appropriate conduct in cyberspace have been received with enthusiasm in some quarters, and the focus of mistrust in others.

Just outside NSJ is a military facility for semi-autonomous weapons. Last year a number of lethal drones were stolen en route from the factory to the base. While they have not yet been used in an attack, intelligence suggests that they may be in the hands of a foreign terrorist group. Information identified by NSJ's autonomous intelligence gathering and reconnaissance unit indicated that bad actors were seeking activation keys for the drones in underground networks. The only remedy was to invalidate all the keys in the relevant range. The intelligence unit has now been set to work on identifying any chatter that may suggest the terrorists are looking for a key generator. Attribution is proving difficult, especially since the advent of software defined ephemeral networks (5/6G). There have also been attempts to alter the code and training data of the self-learning missile system housed at the base.

Fully autonomous weapons systems are still being debated internationally. For now, there is a moratorium on their testing. While New San Joban is abiding by the terms, allegations have been made in the United Nations Security Council that East San Joban is not. Amid escalating tensions in the region, other countries are threatening to withdraw their support for a ban.

Like most local authorities, the city council of NSJ is struggling to store and manage the amount of data generated in the last thirty years. A local tech company has invited them to trial its solution for storing data in DNA. While this promises much greater efficiency, especially for information that can be archived, some citizens are opposed to this use of biological material, however synthetic. Religious groups and conspiracy theorists have been particularly vocal, for different reasons.

As attacks on bionics and the emerging trend for malware in programmable material have demonstrated, members of the public are understandably nervous about cyber threats with potential to harm their physical integrity.

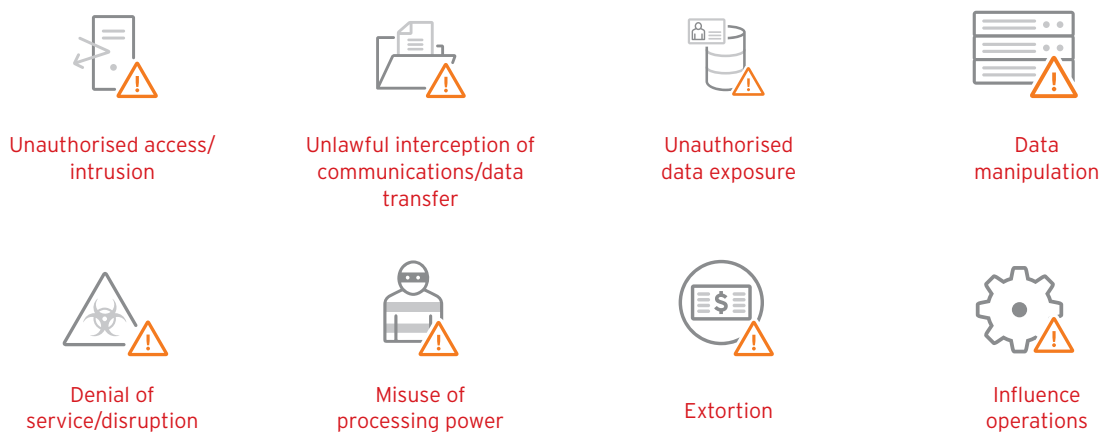
Progress towards quantum processing continues apace. Quantum decryption of the 2048-bit RSA algorithm is nigh. And while local authorities have had several years' warning to transition to post-quantum cryptography, lack of standardisation or guidance on when to jump, and to where, has created confusion, over-reliance, and, in some cases, overspend on third party solutions, and a lack of preparedness in some parts of the world. Amid conflicting information, Resila is keeping her fingers crossed for NSJ, and is hoping that it will be a damp squib, just like Y2K when she was a child.



**“ In the age of the Massive Internet of Things (MIoT) and 5G, everything is connected via a SIM. The interconnection of a massive number of devices and sensors has spawned new types of attacks, and some new vectors for old attacks. ”**

# Cyber Threats

The criminal activities envisaged in the scenario narratives may be grouped into the following general categories:



As is the case in 2020, a single cyber threat business model may engage in a number of these activities in sequence or simultaneously. For example, the current trend for targeted ransomware with double extortion requires unauthorised access to exfiltrate data, and denial of service as leverage; but also secondary leverage in the form of a threat to publish exfiltrated data.

In line with the previous iteration of this exercise, to no small degree the activities above represent an evolution of threats already manifest. What changes on the road to 2030 – at least as they emerge from the scenario narratives constructed – are the enablers, the targets, and the potential impact of attacks.

The next decade promises to be one in which repetitive operations are automated more than ever before, and machine learning advances to the extent that all organisations and sectors of society will make use of artificially intelligent tools. This inevitably will include bad actors, be they individuals, criminal enterprises or nation states. In particular, it is reasonable to assume that highly automated reconnaissance, target selection, penetration testing and delivery will be attractive to cybercriminals, and that they will seek to maximise the effectiveness and efficiency of their efforts by using tools that are capable of unsupervised learning. Based on what we already know of criminal markets for Crime as a Service (CaaS), we may expect to see illicit retail of AI-enabled tools that offer individuals with little or no specialist technical skill the opportunity to run a cybercriminal enterprise. This may fuel a boom in the numbers of that class of cybercriminal who is more herder/manager than hacker.

AI-powered attacks will inevitably be supported by more advanced obfuscation techniques, themselves perhaps boosted by AI. Self-learning fast-flux tools for evading data capture and attribution are the logical evolution of existing anonymisers. But as in the current debate around AI-powered cyber defence, ‘hands-off’ cybercrime is likely to provide unintended opportunities for its disruption if its operations are not entirely understood by its operators.

Interference with the correct operation of AI will likewise provide criminals with their own opportunities. Complex attacks involving the manipulation of datasets from which AI will learn would engineer adverse outcomes, including safety issues and robot misbehaviour. Such methods may be of particular interest to well-resourced corporations or nation states looking to gain competitive advantage by more sophisticated means than intellectual property theft.

At the same time, the scenarios highlight the potential for data manipulation to have a more direct impact on people and things. Where data is a key feature of supply chains in 2030 – for example, in food production or drug delivery – altered ingredients or instructions could lead to physical harm. In such a scenario, cyber attacks would result in recalls of physical products. There would also be scope for exploitation by extortionists by means of a modus operandi not dissimilar to the proverbial glass in supermarket baby food. Meanwhile, the physical connection of human bodies to the internet by means of implants or prosthetics raises the possibility of disruption or damage to physiology. Adoption of Brain-Computer Interfaces (BCIs) will likewise present challenges for the integrity of neurological processes. A simple transfer of the established threats of unauthorized access, denial of service, exfiltration and ransomware to sensors embedded in tissue serves to illustrate the threat, which for some people could prove nothing short of deadly.

In a world in which information is delivered in citizens' immediate line of sight by means of immersive technologies and Heads Up Displays (HUDs), as opposed to a screen at arm's length, data manipulation may be harnessed in the service of influence operations and disinformation. Subsequent iterations of Algorithmic Optimisation (superseding SEO), be they benevolent or malicious, may have greater power to alter belief systems. Social engineering as a threat vector may likewise be harder to resist in environments in which the immediacy of experience will prompt quicker reactions and a reduction in critical distance. While doubtless some would argue that mind control via internet-mediated services is already apparent in 2020, information may be much more persuasive in the 2030 envisaged in the scenarios. Further advancements in natural language processing and GANs may also enable criminals to deploy synthetic scams with greater apparent authenticity and humanity.

Threats aimed at things will have billions more connected targets in the guise of the MIoT. Existing IoT botnets have already demonstrated the potential for hijacking processing power. Envisaged in the scenarios is a step further, that of monetizing MIoT compromise. While the notion of street lights phoning premium rate numbers may at first glance seem a little fanciful, it takes its inspiration from the already established criminal enterprise of telecommunications subscription and toll fraud.

In a truly MIoT environment, successful cyber attacks will result in disruption not only to manufacturing and logistics, but also to transportation, healthcare, education, retail, and the home environment. In the context of additive manufacturing, specifically 4D printing, disruption or denial of service to sensors could result in products not changing shape or state as intended.

Moreover, the 2030 envisaged in the scenario narratives is one in which edge processing and analytics empower things to be self-routing and self-altering. In this future, also one of increased self-learning and autonomy for algorithms, our appreciation of insider threats may need to evolve. Hitherto understood to refer to a human's risk to an organisation, the insider threat of 2030 could just as easily be an object or an algorithm.


In New San Joban, third party and supply chain compromise is even more prominent than it is in 2020. A world of Everything as a Service (EaaS) is one in which the compromise of a giant cloud-based service provider is an even greater prize, and promises greater impact than unauthorised access to a single corporate network. Meanwhile, current signals of components that are shipped with malware pre-installed find their counterparts in the operating environments depicted in the scenario narratives as infected things with distributed impact.

When connected things are on the ocean floor and in orbit around the Earth, there is potential for cybercrime to reach further than ever before. 5G and 6G will enable this truly massive number of connections and significant advancement in IoT deployment that will perhaps be most visible in urban environments. The extended coverage of 5G and 6G coupled with a proliferation of sensors will also open the door for cyber threats that operate on a grander scale. Meanwhile the seamless connectivity envisaged raises the possibility of more effective location-based targeting of attacks with potential to lock down or commandeer the integrated services and networks of an entire city or state. The future envisaged in the scenarios is one in which next-generation wireless technologies will provide opportunities for attacks that are more pervasive and at the same time geographically more specific.

Increasing dependence for connectivity on low earth orbit satellites will inevitably make these an attractive target for financially or ideologically motivated attack. Interest in autonomous vehicle interference and hijacking has already been demonstrated, and it is reasonable to expect that interest to intensify in the next decade. As suspicion of 5G technology has already illustrated, resistance to emerging technologies can manifest in physical destruction. A world in which this technology not only enables a proliferation of things that gather data and report and respond to stimulus, but also facilitates the evolution of AI, is one in which we might expect to see physical and cyber attacks with the aims of halting or slowing technological progress. In some jurisdictions, discontent with greater personal data capture and surveillance may give rise to public disorder.

In the world described in the scenario narratives, new grey and criminal retail markets emerge. Resistance to surveillance while at work may give rise to AI-powered tools for gaming corporate productivity monitoring that boast realistic audio-visual representations of employees. In this context, identity theft will also be reloaded with the ability to pose convincingly as another person in government, corporate and consumer settings.

In countries with a single national ID integrated across a range of services, credentials will be of high value to criminals. Access credentials for digital twins may enable criminals to conduct advanced reconnaissance of organisations' networks and services and even development-stage testing of malicious activity. Meanwhile, a further increase in lifestyle data captured by wearables, implants and other objects containing sensors will be ripe for exploitation by next-generation consumer surveillance tools. There is potential for cyber-enabled violence to be facilitated by smarter stalkerware.



**“ Increasing dependence for connectivity on low earth orbit satellites will inevitably make these an attractive target for financially or ideologically motivated attack. ”**

For all that the scenario narratives create space for new threat vectors and criminal modi operandi, equally there is room for older style attacks to persist. For example, an enduring presence of physical retail outlets speaks to the continued viability of point of sale (PoS) compromise. As imagined in New San Joban, such activity would disproportionately affect older generations and the technologically less advanced.

# Implications for Cybersecurity Stakeholders

The scenarios presented in Section 3 raise a number of considerations for today's stakeholders and decision makers. These include, but are not confined to, the following.

## Changes to the Business of Cybersecurity

In a future of AI cyber attack, defence and incident response, the role of humans will have evolved. Thresholds for escalation to human review will be raised, but will also be affected by regulatory considerations, including data protection and breach notification requirements. As depicted in the scenario narratives, security professionals will focus on strategy and policy setting, performance monitoring, and explaining actions taken. The last of these predicates a need for AI-powered security tools to be explainable, while the shift in core activities presumes a change in human skill sets: as one survey participant remarked, "Within 5 years SOC [security operations centre] analysts will be data scientists".

Continuation of the trend towards outsourcing security and IT operations aligns with the assessment of the survey participants, 63% of whom agreed with the statement that by 2030, "cybersecurity will largely consist of AI offense and defense. Every day will be zero-day" (Q.12), and 66% that "AI will report a breach to the authorities before human data controllers even know about it" (Q.20). The speed of AI cyber attacks poses a particular challenge to timely attribution, particularly in cases where self-learning obfuscation tools frustrate attribution efforts. In a scenario in which attribution is all but unfeasible, enforcement against bad actors risks being confined to the pursuit of the careless and unsophisticated on the one hand, and the dedication of resources to investigating attacks bearing the hallmarks of state sponsorship on the other. Given that state-sponsored groups are most likely to have the resources to make use of next-gen criminal security tools, we may see an extension of the already familiar race of tool and technique development, which pits investigators' and criminals' wits against each other.

At a more general level, an AI offence/defence model necessarily accords greater prominence to the activities of prevention and incident response than to enforcement. An AI-powered cyber attack is under no obligation to constrain its tactics, techniques and procedures (TTPs) to methodologies previously imagined and utilised by human-driven attacks. We will be entering an extended period of experimentation and exploration in novel attack methodology. Threat intelligence is of greater value in this context, be it technical or human. It also prompts a further question - previously raised in the Project 2020 white paper - concerning the roles and responsibilities of the various cybersecurity stakeholders. For example, in a world where the prospect of enforcement through attribution has further diminished, law enforcement personnel could refocus their efforts on infiltrating criminal groups for the purposes of disruption and human intelligence development.

## Death of the Perimeter: Security and Identity on the Edge

A future of billions of objects connected to 5G and 6G (MIoT), edge processing and analytics, truly distributed/cloud computing, and Everything as a Service (EaaS) demands an end to cybersecurity's historical preoccupation with perimeters and network-based protections. Computing and security paradigms are already evolving to meet these emerging requirements, accelerated by 2020's rapid and unprecedented shift to remote working. The increasing popularity of the Secure Access Service Edge (SASE) concept, including Software-defined Wide Area Networks (SD-WAN), Secure Web Gateways (SWG), Cloud Access Security Brokerage (CASB), and Firewall as a Service (FWaaS), effectively acknowledges the impending obsolescence of the physical network security model. Zero Trust approaches, meanwhile, align with a recognition of the growing irrelevance of perimeters to organisational security.

Greater focus on Identity and Access Management (IAM) is therefore a logical move for information security functions. The world of the scenario narratives contains greater integration of digital identities across devices and services, synthetic identities that do not map to offline humans or devices, and even more opportunities for humans to alter their identities according to the situation. In such a future, effective security solutions will need to be cognizant of and provide for this complexity.

## Embodied Cybersecurity

In the event that immersive technology is adopted to the extent seen in New San Joban, authentication via Heads Up Display – for example, via iris recognition – may become a more widespread means of human authentication. The potential psychological and emotional impact of threats and cyber-enabled violence delivered via immersive technology may result in the information security workforce of tomorrow working more closely with mental health specialists on emergency response, and being called upon to analyse and present data pertinent to adverse experiences: lawsuits alleging psychological harm or emotional distress as the result of IT compromise and delivery of inappropriate content cannot be ruled out. Similarly, information security professionals will be required to investigate physical injuries and deaths involving connected healthcare devices: digital evidence will be scrutinised routinely in the course of an autopsy; CISOs may be called to give testimony at coroner's courts. As one survey participant observed, cyber-physical security will no longer apply solely to critical infrastructure: "The cyber physical risk that we see in OT [Operations Technology] and control systems will be prevalent everywhere. A cyber attack that could cause physical or environmental harm greatly supersedes the impact of a run of the mill data breach. Losing humans not data..."<sup>3</sup>

---

<sup>3</sup> Free text response to Q.35: What will keep information security professionals awake at night?

That said, the scenario narratives posit that not everyone in society will be enthusiastic about the idea of being physically connected to the internet. Current suspicion from some quarters of advances such as 5G and COVID vaccines – of which the conspiracy theory that the vaccine will come with a free tracking microchip is perhaps the most notable – illustrates the ease with which tech can be associated with physical harm. Outside of medical use cases, we may well see a generational divide similar to that in New San Joban, with younger people much less squeamish about the prospect of bodily digital enhancement. For the cybersecurity community, this translates to greater risk of compromise in this target group and the medically vulnerable.

## Everything is Cyber Now

Already in 2012, the scenarios for Project 2020 foresaw a convergence between cybersecurity and national security, and a complex interaction between cybersecurity and international relations. Current reporting reflects the changing nature of nation state and state-sponsored cyber threat activity. Meanwhile, countries and regions are increasingly focused on preserving their digital sovereignty, and techno-nationalism has become a key geostrategic tool of some of the world's most powerful nations. As the scenario narratives demonstrate, restrictions on supply chains have the potential to impact not only on the speed of adoption of emerging technologies, but also on the ability to secure them. Countries acting now to foster home-grown innovation in cybersecurity will weather the challenges of this possible future better than those dependent on foreign suppliers.

In such a future, information security professionals can expect even closer scrutiny of their procurement choices, and potentially to have less choice than before. In addition, the distinction between cyberspace governance – determining sovereign jurisdiction and the rules of cyber operations – and internet governance (content regulation) appears to be blurring further, and may be at risk of vanishing entirely without multilateral clarification. With continued forward movement, the trends for techno-nationalism and digital sovereignty will pose not insignificant challenges to truly open markets, and will remove forever the prospect of a truly global internet.

## Technological Disparity

The scenarios in this paper were consciously constructed to reflect a society in which emerging technologies have been subject to the fullest adoption possible. The characterisation of New San Joban as an international pioneer created sufficient space to consider a larger range of technological applications and cyber threats. It is unrealistic in the extreme to assume that the advances described in the narratives will be available to the same degree in all parts of the world. Indeed, almost half of survey participants were pessimistic even about the world's population being connected to the internet in the next ten years. Potentially revolutionary technologies such as quantum computing will likewise not suddenly be available to all.

The world's largest technology companies and best-resourced research institutes are the pioneers in this space and are preparing to lease quantum processing as a service. The balance of quantum power will therefore be held in a comparatively small number of geographical locations, with a trickle down to those who can afford it, raising the possibility of even greater disparity between the technological 'haves' and 'have nots'. Such disparity would also manifest in an exacerbation of the cybersecurity capacity gaps already discernible in 2020.

## Popular Resistance – Moral and Ethical Focus

In recent years, high profile data breaches and privacy scandals have demonstrated the global public's moral and ethical expectations of technology. Unethical supply chains and decision-making in nascent AI have made headline news, with the promise of much more to come. Even selecting the correct people to consider issues of tech ethics has become a matter of public interest and controversy. The scenario narratives envisage a future in which technology has been harnessed to combat global challenges such as air and marine pollution, large corporations have achieved carbon negativity targets, and energy is produced locally. There is no reason to expect that the world's population will be desensitised to these issues in the coming decade. On the contrary, whether in relation to privacy, environmental concerns, or human rights, it is likely that there will be even greater emphasis placed on developing technology, including that used by information security professionals, on doing the 'right' thing. Expertise in ethics may well become a highly-prized technology development asset over the next decade.


## Mind the Regulatory Gap

The scenario narratives describe the possibilities and risks of a truly AI-enabled life, which will be more intrusive by dint of the sheer frequency and extent of its data gathering. This prompts the question of whether existing data protection regimes will be fit for this kind of future, or whether additional legislation will be required to protect citizens' from ubiquitous surveillance. An additional consideration concerns the volume of data that will have been generated by 2030. Regulation of data processing and storage will need to be complemented with requirements for archiving, aging and weeding, with time limits where appropriate. Personal archiving and legacy services may emerge to handle this, as part of a commercial privacy management sector.

Instruments governing the use and abuse of AI in relation to consumers, investigatory powers in environments such as smart cities with seamless but ephemeral connectivity, and other activities may be required. The majority (54%) of survey participants agreed with the statement that by 2030 "countries will launch cyber-attacks on each other by mistake, and with no human intervention" (Q.13). The question itself highlights the need for regulation in this space. While it is tempting to assume, with one participant, that "New conventions of war will be established to prevent or mitigate this type of thing," rival proposals for multilateral cyberspace governance in 2020, and a persistent tendency for technological adoption to outpace regulation, would suggest that conclusion of a multilateral agreement by 2030 on the use of Lethal Autonomous Weapons Systems (LAWS) may be optimistic.

## Truth, Trust & Authenticity

From the vantage point of 2020, the accepted notions of truth, trust and authenticity are already under threat. According to popular commentary, we are already in a 'post-truth' society. The world of 2030 depicted in the scenario narratives highlights the need to introduce new measures to assist citizens in distinguishing fact from fiction, and honesty from dishonesty. Delivery of hyper-targeted content in the line of sight may constrain citizens' reactions to what they see - information may be more persuasive simply by virtue of being visual, or perhaps even visceral. AI-driven targeted behavioural advertising may reduce consumer decision-making ability. A lower level of knowledge retention by individuals will put an even greater focus on the knowledge that is accessible. Legitimate applications of synthetic humans in consumer and business settings may reduce the effectiveness of tools that flag inauthentic behaviour based on automated activity, or security measures reliant on authentication of facial features. It may be necessary to make unprecedented efforts to improve citizens' critical thinking, or at least to encourage a 'post-trust' appreciation of truth: live calls from a real-time deepfake of a family member asking for money would be difficult to resist and cannot be ruled out. Equally, in the face of such compelling scam vectors, technical authenticity tools could become more important.



**“ The majority (54%) of survey participants agreed with the statement that by 2030 “countries will launch cyber-attacks on each other by mistake, and with no human intervention.” ”**

# Beyond 2030

A number of technological developments and impacts were deemed to be too ambitious for the timeline of the scenario narratives. The great uncertainty is whether quantum computing will be in mainstream use by 2030, and when it will crack existing encryption algorithms. While it is possible that both of these will happen in the next ten years, its depiction in the narratives as imminent has been a deliberate move to postpone detailed consideration of a technology whose impact may be unprecedented and whose potential is likely to be highly disruptive.

Given the current excitement surrounding Starlink and other low earth orbit initiatives, it was tempting to include in the scenario narratives a larger amount of material on cybersecurity in space. After careful consideration, this temptation was resisted. Situating more of the action in space would have risked detracting from cybersecurity concerns on Earth, which are expected to be more than sufficient to preoccupy the vast majority of information security professionals.

Brain Computer Interfaces (BCI) were deemed to be potentially emerging but not in mainstream use by 2030, outside of medical use cases. Taking the notion of influence operations via Heads Up Displays (HUD) a leap further, targeting of BCIs raises the possibility of thought process compromise - true 'mind control' - that thankfully was beyond the likely time horizon for this iteration of the project. Also relevant to bodily integrity is programmable tissue, not projected to be mainstream by 2030, but inevitably prompting considerations of potential tissue damage and morbidity as a result of safety and security issues.

Touched on in the scenario narratives but not discussed in detail is the notion of non-human agency. In the popular imagination, the concept of rights for robots has been around for at least a century now, certainly since Karel Čapek. The smarter AI becomes, the more we will hear this debate. But there is some way to go before the advent of sentient AI - further than 2030 at least.

# Appendices

## Scenario Method

The scenario narratives and their implications for cybersecurity stakeholders have been elaborated on the basis of a combination of current signals and emerging technological developments, largely following the process used by its predecessor, **Project 2020**, published in 2013.<sup>4</sup> In the first instance, a synthesis of annual cyber threat predictions, published in late 2020, served as a baseline assessment of the threat landscape in 2020. Next, a review of scientific abstracts, patents and open source material relating to emerging technologies was conducted by the research team. This resulted in the identification of potential drivers for change and key uncertainties related to the future of cyber threats and cybersecurity.

Validation of timelines for technological development and of resulting concerns for cybersecurity stakeholders moved online as a result of the COVID-19 pandemic. An invitation-only online survey was distributed to information security, data protection, international relations, criminal justice, and other specialists in the public, private and third sectors. The survey comprised 32 multiple choice questions, each consisting of a statement on possible technological developments by 2030. A total of 101 completed surveys was received. The full list of questions and analysis of results can be found at the end of this document.

In addition, the Pulse CISO360 online conference in December 2020 provided an opportunity to conduct a live poll of information security leaders, focused on a subset of the survey questions specific to the future of security operations (QQ.12, 13, 15, 20 & 25). Both the poll results and the accompanying text discussion were incorporated into the timeline validation, and informed the drafting of the scenario narratives.

Technological developments identified as likely by 2030 became transformative features of New San Joban, the city state described in the narratives. By design, the narratives illustrate the interconnectedness of citizen, corporate and government experiences in the cybersecurity ecosystem of 2030, and the relationship of cybersecurity to potential developments in the wider global context. The construction of interconnected scenario narratives enabled the identification of potential cyber threats and criminal opportunities, implications for cybersecurity stakeholders, and key uncertainties in this possible future. These are discussed in Sections 4, 5 and 6 of this white paper.

---

<sup>4</sup> A review by the authors of the methodology and results of Project 2020 can be found at <https://2020.trendmicro.com/review-2020/>

## Timeline Validation

For each of the test statements, participants were asked to choose one of three answers.



### 8. By 2030...Heads Up Displays (HUDs) will be part of us

1. Too ambitious
2. About right
3. Not ambitious enough

**“ Within 5 years SOC [security operations centre] analysts will be data scientists ”**

**Live poll participant,**  
DECEMBER 2020

For each question, a link to a news article provided food for thought, and a free text box afforded the opportunity to explain the choice made. Further free text questions invited participants to identify pertinent technological developments omitted in the preceding statements and the future preoccupations of information security professionals. Statistical returns for the multiple choice questions served to validate the timelines for technological development, and the draft scenario narratives were adjusted accordingly. Particular attention was paid to test statements that were deemed to be insufficiently ambitious for 2030. Free text responses were reviewed individually.

# Survey Questions

Q1.	By 2030...We will print our own food at home.	Q20.	By 2030...AI will report a breach to the authorities before human data controllers even know about it.
Q2.	By 2030...Crops, livestock and fish will be monitored remotely, and farmed/fished by robots.	Q21.	By 2030...Some people will suffer technological unemployment.
Q3.	2030...Daily print media will have gone entirely online.	Q22.	By 2030...Civilians will go into space for fun.
Q5.	By 2030...Small and medium sized enterprises will make use of quantum computing.	Q23.	By 2030...Insurers will profile us without asking us questions about ourselves or our property.
Q6.	By 2030...We will direct several different versions of ourselves at once. Some will have achieved 'digital immortality'.	Q24.	By 2030...Brain computer interfaces will feature in our work and play.
Q7.	By 2030...We will get used to other people looking different every time.	Q25.	In 2030...Quantum-safe encryption will be the preserve of the well-resourced.
Q8.	By 2030...Heads Up Displays (HUDs) will be part of us.	Q26.	By 2030...Supply chains will maintain and fix themselves. Humans will make logistical decisions only when automation makes a mistake. Humans will investigate anomalies.
Q9.	By 2030...We will only meet people face to face to socialize and create.	Q27.	By 2030...Drones will have replaced people and vehicles for shopping, mail and mail order delivery.
Q10.	By 2030...Large swathes of office space will have been repurposed for living and socialising.	Q28.	By 2030...Vehicles with Level 4 autonomy will be widespread.
Q11.	By 2030...AI-powered gene editing will have begun to eradicate diseases.	Q29.	By 2030...Many large manufacturers will have achieved carbon neutrality, and some carbon negativity.
Q12.	By 2030...Cybersecurity will largely consist of AI offense and AI defense. Every day will be zero-day.	Q30.	By 2030...A machine will make decisions about when to administer machine-discovered drugs to you. A machine will deliver them. A machine will administer them. No humans will be involved.
Q13.	By 2030...Countries will launch cyber-attacks on each other by mistake, and with no human intervention.	Q31.	By 2030...Physical retail outlets will be for the nostalgic.
Q14.	By 2030...In some countries, wars will be fought largely by autonomous weapons.	Q32.	By 2030...Decentralised autonomous organisations will challenge both national sovereignty and corporate hegemony.
Q15.	By 2030...Blockchain will have solved the current problems of data integrity and assurance.	Q33.	What have we missed? What else should we be considering for the world of 2030?
Q16.	By 2030...Large tech companies will have dropped business models that rely on targeted advertising.	Q34.	The single biggest change between now and 2030 will be...
Q17.	By 2030...Public figures will use evolved deepfake technology to communicate with the public, rather than doing it in person.	Q35.	What will keep information security professionals awake at night?
Q18.	By 2030...In person, face to face, political debate and campaigning will be a historical artefact.		
Q19.	By 2030...It will no longer be necessary to learn foreign languages.		

# Survey Responses

Question	Too Ambitious	About Right	Not Ambitious Enough
Q1. By 2030...We will print our own food at home	67.71%	27.08%	5.21%
Q2. By 2030...Crops, livestock and fish will be monitored remotely, and farmed/fished by robots	17.89%	67.37%	14.74%
Q3. By 2030...Daily print media will have gone entirely online	23.96%	51.04%	25.00%
Q4. By 2030...The world's population will be connected to the internet	45.26%	47.37%	7.37%
Q5. By 2030...Small and medium sized enterprises will make use of quantum computing	55.79%	37.89%	6.32%
Q6. By 2030...We will direct several different versions of ourselves at once. Some will have achieved 'digital immortality'.	64.21%	25.26%	10.53%
Q7. By 2030...We will get used to other people looking different every time	43.01%	44.09%	12.90%
Q8. By 2030...Heads Up Displays (HUDs) will be part of us	26.32%	58.95%	14.74%
Q9. By 2030...We will only meet people face to face to socialize and create	39.36%	45.74%	14.89%
Q10. By 2030...Large swathes of office space will have been repurposed for living and socializing	11.46%	68.75%	19.79%
Q11. By 2030...AI-powered gene editing will have begun to eradicate diseases	37.50%	51.04%	11.46%
Q12. By 2030...Cybersecurity will largely consist of AI offense and AI defense. Every day will be zero-day	23.16%	63.16%	13.68%
Q13. By 2030...Countries will launch cyber-attacks on each other by mistake, and with no human intervention	29.47%	54.74%	15.79%
Q14. By 2030...In some countries, wars will be fought largely by autonomous weapons	32.29%	55.21%	12.50%
Q15. By 2030...Blockchain will have solved the current problems of data integrity and assurance	48.39%	36.56%	15.05%
Q16. By 2030...Large tech companies will have dropped business models that rely on targeted advertising	45.26%	32.63%	22.11%
Q17. By 2030...Public figures will use evolved deepfake technology to communicate with the public, rather than doing it in person	32.29%	51.04%	16.67%
Q18. By 2030...In person, face to face, political debate and campaigning will be a historical artefact	64.21%	29.47%	6.32%
Q19. By 2030...It will no longer be necessary to learn foreign languages	38.95%	52.63%	8.42%
Q20. By 2030...AI will report a breach to the authorities before human data controllers even know about it	15.96%	65.96%	18.09%
Q21. By 2030...Some people will suffer technological unemployment	2.15%	61.29%	36.56%
Q22. By 2030...Civilians will go into space for fun	38.54%	52.08%	9.38%
Q23. By 2030...Insurers will profile us without asking us questions about ourselves or our property	14.58%	61.46%	23.96%
Q24. By 2030...Brain computer interfaces will feature in our work and play	48.96%	41.67%	9.38%
Q25. In 2030...Quantum-safe encryption will be the preserve of the well-resourced	20.83%	60.42%	18.75%
Q26. By 2030...Supply chains will maintain and fix themselves. Humans will make logistical decisions only when automation makes a mistake. Humans will investigate anomalies	16.67%	71.88%	11.46%
Q27. By 2030...Drones will have replaced people and vehicles for shopping, mail and mail order delivery	52.63%	37.89%	9.47%
Q28. By 2030...Vehicles with Level 4 autonomy will be widespread.	24.47%	62.77%	12.77%
Q29. By 2030...Many large manufacturers will have achieved carbon neutrality, and some carbon negativity	40.00%	42.11%	17.89%
Q30. By 2030...A machine will make decisions about when to administer machine-discovered drugs to you. A machine will deliver them. A machine will administer them. No humans will be involved	53.13%	40.63%	6.25%
Q31. By 2030...Physical retail outlets will be for the nostalgic	41.05%	49.47%	9.47%
Q32. By 2030...Decentralised autonomous organisations will challenge both national sovereignty and corporate hegemony	36.84%	47.37%	15.79%

Fig.3 Results of invitation-only online survey on plausible technological developments, captured 02/12/2020

Question	Too Ambitious	About Right	Not Ambitious Enough
Q12. By 2030...Cybersecurity will largely consist of AI offense and AI defense. Every day will be zero-day.	27%	58%	15%
Q13. By 2030...Countries will launch cyber-attacks on each other by mistake, and with no human intervention.	38%	38%	24%
Q15. By 2030...Blockchain will have solved the current problems of data integrity and assurance.	53%	21%	26%
Q20. By 2030...AI will report a breach to the authorities before human data controllers even know about it.	40%	40%	20%
Q25. In 2030...Quantum-safe encryption will be the preserve of the well-resourced.	17%	72%	11%

Fig.4 Results of a live 'lightning' poll conducted with delegates of CISO 360's online conference, December 2020

# About the Author

## Dr Victoria Baines



Dr Victoria Baines is a leading authority in the field of online trust, safety and cybersecurity. She frequently contributes to major broadcast media outlets on digital ethics, cybercrime, and the misuse of emerging technologies, including virtual reality and artificial intelligence (AI). Her areas of research include electronic surveillance, cybercrime futures, and the politics of security. She also provides research expertise to a number of international organizations, including Interpol, UNICEF, and the Council of Europe.

Victoria is co-host of the award-nominated Cyber Warrior Princess podcast, demystifying cybersecurity for a popular audience. She regularly addresses both specialist and non-specialist audiences and has been named as one of the top 25 women in cybersecurity (IT Guru & SC Magazine).

For several years Victoria was Facebook's Trust & Safety Manager for Europe, Middle East, and Africa. Her work focused on operational support to law enforcement, and strategic engagement with policy makers on criminal activity online. Before joining Facebook, Victoria led the Strategy team at Europol's European Cybercrime Centre (EC3), where she was responsible for the EU's cyber threat analysis. She designed and developed the iOCTA, Europe's flagship threat assessment on cybercrime, and authored 2020, scenarios for the future of cybercrime that were the basis for a successful short film series of the same name.

Prior to this, Victoria was Principal Analyst at the UK Serious Organized Crime Agency (SOCA), the forerunner of the National Crime Agency. She began her career in law enforcement in 2005 as a Higher Intelligence Analyst for Surrey Police. In 2008, the International Association for Law Enforcement Intelligence Analysts recognized Victoria's work with a global award for outstanding achievement.

Victoria serves on the Advisory Boards of cybersecurity provider Reliance ACSN and the International Association of Internet Hotlines (INHOPE) and is a trustee of the Lucy Faithfull Foundation. She is a graduate of Trinity College, Oxford and holds a doctorate from the University of Nottingham, UK. She is a Visiting Fellow at Bournemouth University School of Computing, a former Visiting Research Fellow at Oxford University, and was guest lecturer at Stanford University in 2019 and 2020.

# About the Author



**Rik Ferguson,**

Vice President Security Research,  
Trend Micro

Researcher, writer, filmmaker, and presenter Rik Ferguson is the Vice President of Security Research at Trend Micro. Rik's research into the murky world of cybercrime and the cloudy future of technology sees him advise law enforcement, governments, and large enterprises alike. He is also a Special Advisor to Europol's European Cyber Crime Centre (EC3), a multi-award-winning producer and writer, and a Fellow of the Royal Society of Arts. In April 2011, Rik was inducted into the Infosecurity Hall of Fame.

A recognised futurist, Rik is actively engaged in research into online threats and the cybercriminal underground. He also investigates the wider implications of new developments in Information Technology, their impact on security, both for the enterprise and for society as a whole, publishing papers, articles, videos and participating in thought-leadership initiatives. Rik has presented his findings at many global events such as RSA, Mobile World Congress, Milken Institute, Virus Bulletin, RUSI and the e-Crime Congress, and is often quoted by media around the world.

With over 25 years of experience in information security, Rik has been with Trend Micro since 2007. Prior to assuming his current role, he served as Security & Privacy Infrastructure Specialist at EDS, where he led the security design work for government projects related to justice and law enforcement and as Senior Product Engineer at McAfee focused on network security, intrusion prevention, encryption, and content filtering

Rik Ferguson holds a Bachelor of Arts degree from the University of Wales and has qualified as a Certified Ethical Hacker (C|EH), Certified Information Systems Security Professional (CISSP), and an Information Systems Security Architecture Professional (ISSAP).



© 2021 Trend Micro Incorporated and/or its affiliates. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.

[WP01\_Project 2030\_White Paper\_210505US]

