サイバーセキュリティの未来シナリオ

Dr Victoria Baines & Rik Ferguson

Endorsed by:
ICC UNITED KINGDOM
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

TREND MICRO

はじめに

毎年、調査結果を集計したレポートは多数発表されており、その結果を未来の予測につなげようとするものもかなりありますが、「Project 2030 – サイバーセキュリティの未来シナリオ」のように示唆と洞察に富むレポートは希少です。

本レポートの著者である Victoria、Rik の両氏は、今からわずか 9 年後に人々の生活がどのようなものになっているかを描き、人々、ビジネス、国家の観点から見たテクノロジの影響というレンズを通して、サイバーセキュリティの全体像を見据えています。

サイバーセキュリティに関するレポートの多くは、ウィンストン・チャーチルの言葉を借りれば恐怖の総和、すなわち事実と数字の無味乾燥な羅列に過ぎません。Project 2030 はそれとはまったく異なります。

もちろん、Project 2030 が推測する未来がここに述べられたままの形で実現することはないでしょうが、ほぼ確実に実現しそうな要素はいくつもあります。たとえば、ますますつながりを強めていく人々に「ディープフェイク」が及ぼす影響、自動化による製造業の劇的な変化、サプライチェーンのセキュリティ問題などです。

最も明瞭に示されているのは、私たちがテクノロジを介して互いのつながりをさらに強めていけば、サイバーセキュリティの問題が政策目標としてだけでなく、一般社会にとってもますます重要になることです。これは私たち皆がある程度は知っていることですが、このレポートがとても大きな説得力をもって示しているのは、今日のサイバーセキュリティの問題と、その問題に私たちがどう対処するかが、明日の私たちの健康と幸せを守るために不可欠である理由です。

テクノロジが今日提示している可能性は、ほんの数年先のそれのごく一部に過ぎません。本レポートから考えさせられることは非常に多く、行動を起こすきっかけにもなるはずです。ICC United Kingdom が国際的なサイバーセキュリティ政策にますます積極的に取り組んでいる理由はまさに、これがリスクを最小化して健全な成果の達成を促す、人類共通の未来の機会を実現するための鍵であるからです。

「Project 2030 – サイバーセキュリティの未来シナリオ」を推奨できることは、ICC United Kingdom の誇りです。

ICC UNITED KINGDOM
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

Project 2030 について

> 「人間はイノベーションというものが本当に不得意です。私たちはどうしてもテクノロジ変革の短期的な影響を過大評価し、長期的な影響を過小評価してしまいます」
>
> ライブ投票参加者、2020年12月

Project 2030は、トレンドマイクロの研究イニシアチブです。その目的は、サイバー犯罪の未来を予測し、政府、企業、市民が今後10年間を見据えて難題と機会に対応する準備を整えられるようにすることです。

ここに示すシナリオは、今後10年間にわたる進展の全体像を表すものではありません。これらのシナリオは考えられる中期的なテクノロジの発展を描いたものであり、個人、製造業者、国家機構の観点から見たサイバー脅威の影響に重点を置いています。述べられている事象と展開は、全世界で必然的に起こるのではなく、世界の一部地域で起こり得ることとして考案されたものです。これらは、現在の脅威の分析、情報セキュリティ、データ保護、法執行、国際関係の各分野における専門家の意見、新興テクノロジの広範なホライズンスキャニングを参考に発案されたものです。

著者は、テクノロジのタイムラインに関するライブ投票の実施をご支援いただいたPulse ConferencesのSara Hook氏、アンケート回答の募集をご支援いただいたNeil Walsh氏、ナノメディシンの未来に関する専門的なアドバイスをご提供いただいたDamien Batchelor氏に感謝いたします。

2020 年からの展望

国際機関および大手サイバーセキュリティプロバイダから発表された脅威レポートを総合することで、2020 年のサイバー犯罪による脅威のベースラインを容易に見極めることができました。国際機関によって特定されたサイバーセキュリティエコシステムの脅威、イネーブラ、その他の特徴は以下のとおりです。

脅威とベクトル		
敵対的AI	DDoS	不正なUSBの郵送
ボットネット	ドキシング／情報漏えい	物理的操作／損傷／損害
ビジネスメール詐欺	高プロファイルデータ損失	ランサムウェア（標的型、高額、サードパーティ攻撃）
ビジネスプロセス詐欺	印象操作／偽情報	リモートアクセス型のトロイの木馬（RAT）
クレデンシャルスタッフィング	インサイダー脅威	SIMスワップ
サービスとしての犯罪（Crime as a service）	IoT侵害またはDoS／エッジ攻撃	スミッシング
クリプトジャッキング	ATM/PoSへの論理攻撃	フィッシング（テーマ／スピア／ホエーリング）
サイバースパイ	不正アプリ	SQLインジェクション
データを盗むトロイの木馬（Emotet）	不正ドメイン	
Webエクスプロイト	サプライチェーンおよびサードパーティに対する侵害	

イネーブラと標的		
クラウド／仮想化	モバイル	正当なビジネス構造／ツールの悪用
犯罪インフラ（防弾ホスティング）	犯罪者が身を隠すための新しい手段	ソーシャルメディア
便乗犯罪	プライバシー強化ウォレット	ディープフェイク
ダークウェブの進化／再生	ソーシャルエンジニアリング	
オンライン金融サービス	パッチ未適用／サポート終了／レガシーアプリケーション	

エコシステム		
自動検出	便乗犯罪	新たな攻撃者

図 1：選定された国際機関から報告された 2020 年のサイバー脅威の一般的な特徴[1]

[1] 欧州刑事警察機構の「Internet Organised Crime Threat Assessment 2020」、ENISA の「Threat Landscape 2020」（Year in Review、Threat Intelligence、Emerging Trends の各レポート）、国際刑事警察機構の「COVID-19 Cybercrime Analysis Report」の手作業によるレビューに基づく。

2020 年のサイバーセキュリティ業界における脅威予測の一般的な特徴は、以下のようなグループに分かれています。

脅威とベクトル		
API攻撃	持続的標的型攻撃（APT）	IoT関連の攻撃
ランサムウェア／二重の脅迫		

イネーブラと標的		
5Gおよび通信	クラウドおよびエッジ	新型コロナウイルスに便乗した攻撃
自動化と人工知能	テレワーク／オンライン授業の影響	ディープフェイク
レガシーの脆弱性		

エコシステム		
サイバー犯罪ギャングの結託	セキュリティの自動化	ユーザのプライバシー
法規制および法執行の活動	パッチウィンドウの短縮	

図 2：選定されたサイバーセキュリティプロバイダから報告された 2020 年のサイバー脅威の一般的な特徴[2]

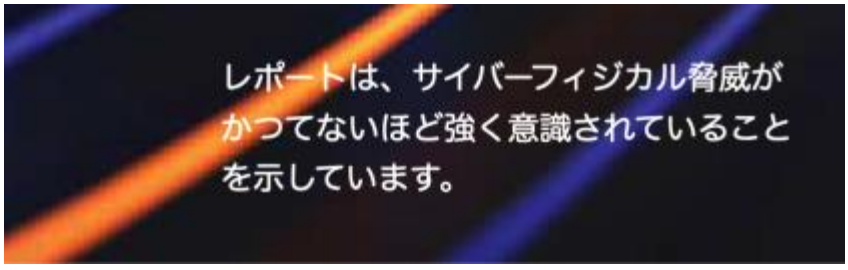
この簡易レビューの目的は、シナリオに対する脅威のベースラインを可能な限り完全なものにすることでした。したがって、国際機関の調査結果をサイバーセキュリティ業界のものと比較したり、それぞれの特徴を同等なカテゴリにまとめたりすることは試みませんでした。それよりも、特定された脅威とベクトル、イネーブラと標的、現在のサイバー脅威エコシステムの特徴をすべて、シナリオの作成時に考慮に入れました。結果として、図 1 と図 2 に列挙されている項目の間にはかなりの重複があります。たとえば、図 2 に示した、国家による、または国家支援型の持続的標的型攻撃（APT）と業界で説明されているものは、図 1 では国際機関によってサイバースパイと呼ばれているものと対応付けられます。これらは別々の用語で表現された同じ脅威です。

新型コロナウイルスのパンデミックは、2020 年のサイバー脅威レポートに必然的に大きな影響を及ぼしています。パンデミックに便乗した攻撃は、テーマを設定したフィッシング、スミッシング、サイバー詐欺として表面化しているだけでなく、国家を舞台にワクチン研究の侵害が試みられたことも報告されており、長年続いているサイバー便乗犯罪の流行に拍車を掛けています。ビジネスと教育の急速な仮想化も同様に、業界と国際機関が揃って主要な状況依存の脆弱性および攻撃ベクトルと見なしていました。本書で紹介するシナリオは、特定のテクノロジが加速度的に主流化していることを背景として作成されたものです。たとえ

[2] BeyondTrust、Checkpoint、FireEye、Fortinet、Kaspersky、LogRhythm、Symantec、トレンドマイクロ、および WatchGuard からの脅威レポートの手作業によるレビューに基づく。

ば Zoom 爆撃のような、現在行われている迷惑行為は、2030 年に至る過程で新興テクノロジが犯罪者に悪用されることを示唆しています。

特に業界のレポートは、サイバーフィジカル脅威がかつてないほど強く意識されていることを示しています。かつては主に重要インフラストラクチャに対する脅威の面で考えられていた、人間のセキュリティが依存するモノ（IoT）とシステムのハッキングが、2020 年のサイバー脅威予測では大きく取り上げられています。この理由としてある程度考えられるのは、自動車のサイバーセキュリティがより本格的に注目されるようになったことでしょう。大きく報道された、パンデミックと戦う病院に対するランサムウェア攻撃も、身体的危害につながるサイバー脅威の未来の展開を示唆する犯罪でした。ランサムウェア攻撃を受けた後に死亡したドイツ人市民について殺人罪で捜査することが発表された一件は、おそらく 2020 年の最も注目すべき事例でしょう。



業界と国際機関の両方のレポートで目立っていた点は、印象操作と偽情報、サイバースパイ、APT、脅迫（ランサムウェア）といった形態を問わず、国家と国家以外のサイバー犯罪者の境界が曖昧になっていることの認識です。これと関連して懸念されているのは、特にサプライチェーンと調達に関して、サイバーセキュリティがどの程度まで戦略地政学的な問題になってきたかということで、これは当然ながら業界レポートでより明確に述べられています。サイバーセキュリティ業界の予測に加え、国際機関のレポートには、未来を見据えた脅威の検討もある程度は盛り込まれていました。たとえば、脅威ベクトルおよびイネーブラとしてのディープフェイクと 5G の利用は、2020 年にはまだ主流ではありませんでしたが、レポートにはこれらに関する言及がありました。

Project 2020 のために脅威レポートを総合する作業もそうでしたが、このように先を見越して準備をしておくことが、継続的なテクノロジの発展を背景に、犯罪者が一定数のテクノロジの悪用を展開するという中期的な未来を想定するために役立ちます。

2030 年のシナリオのストーリー

a. 市民 – Resila

ニュー・サン・ジョバンで生まれた Resila はずっとこの街で育ちました。両親は前世紀、大学に在学中に出会いました。Resila が 2 人の子どもたちを産んだのもこの街でした。世界でも最先端のテクノロジを誇るこの街の市民である Resila は、さまざまな理由でテクノロジのありがたみを実感しています。

Resila はショッピングが好きではありません。子どもの頃、毎週土曜日になると、彼女の母親は Resila を連れてスーパーマーケットへ出かけました。通学用の新しい服や靴を買うため、毎年街中を引き回されてあれこれ試着させられました。でも Resila の子どもたちにはそんなことをする必要は一切ありません。替えの服がぴったりのサイズで必要なタイミングに用意できるよう、子どもたちの服に内蔵されたセンサーが常に仕立て用の寸法を測っているからです。

ウェアラブルセンサーは家族に必要な栄養を特定するのにも役立っており、ビタミンやその他の栄養分が不足していれば教えてくれます。Resila は、食物繊維の摂取を増やし、脂肪と炭水化物を減らす必要が生じると、買い物カゴを自動的に調整してサプリメントを注文できるサービスを利用しています。そのオンラインマーケットの商品棚には、許可された品物や、Resila に役立つ品物だけが陳列されています。アルコールや砂糖など、特定の商品を摂取しないよう医療データによって警告されている顧客は、ストアのそのセクションをロックして入れなくすることを要求できます。毎日使う食料品や日用雑貨は自動的に再注文され、ドローンで配達されます。

プレミアムサービスを利用すると、これらの栄養面のデータを Resila のかかりつけ医が持つ医療記録やジムのメンバーシップ、睡眠パターンとリンクさせることができ、さらにトイレの便器と接続して胃腸の健康までも管理します。Resila のコンタクトレンズは定期的に彼女の涙液を検査して、ガンや脳卒中、糖尿病など、いくつかの一般的な急性および慢性の症状が出ていないか健康状態を確認します。異常が見られた場合、詳しい検査や相談、治療のため医療機関に予約が入ります。こうしたものに抵抗を感じる層は、代わりに皮膚そっくりのパッチを選んでいます。これは汗の成分を監視して変化を報告するもので、処方薬の継続的な服用にも役立ちます。また DNA プロファイリングも、10 年以上にわたる商業利用により、予防医療に直接的に貢献しています。

3D プリントの技術により、食肉生産の必要もなくなっています。Resila は必要なものを家でプリントするだけです。Resila も最初は半信半疑でした。しかし人々の健康志向と環境へ

の配慮が高まり、輸送コストの増加と化石燃料の段階的な廃止が進んだことによって、流行のレストランに大きな利益をもたらす市場が生まれ、レストランがレシピから収益を得、栄養補助食品を取り入れ、原材料の生産者と連携する仕組みができました。Resila は環境に貢献できることを喜んでいますが、プリントボタンを押す前にレシピをもう一度確認するようにしています。また、公衆の安全に関わる発表には常に目を光らせています。最も人気のあるサブスクリプションサービスが昨年ハッカーに攻撃され、成分リストを書き換えられたことにより、多くの人々が食中毒になりました。

この 10 年間で、医療業界は大きな進歩を遂げました。ウェアラブルデバイスがより高度化され、データと創薬の分野がさらに力を得ました。Resila の父親は、抗凝血剤を服用しています。この世代では珍しいことではありません。以前は血液濃度の計測のため定期的に通院する必要がありました。医師は検査結果に従って薬の用量を調整し、父親に電話で伝えます。連絡を受けた父親は、服用する薬を覚えなくてはなりませんでした。しかし今では、ウェアラブルモニターによって採血と分析が行われ、それに基づいて処方箋が自動的に更新されて、服用指示が自宅の 3D プリンタに送信されます。父親がプリンタで生体認証を済ませると、全体的な投薬計画が分析されて必要量の配合薬が調剤されるので、服用する錠剤の総数が最小限になります。国によってはこのプロセスから人間による検証がまったく省かれているところもありますが、ニュー・サン・ジョバンでは調剤薬の人間による検証が法律で義務づけられています。もちろん、それでも間違いは起こります。Resila の父親はナノロボティクスによる治療を勧められてきましたが、Resila がそれを安全だと考える一方で、父親本人は自分の身体に取り込まれる薬について、自らで調整できる部分を残しておきたいと考えました。

近年では、バッテリーによるエネルギー貯蔵がかなり安価に、効率的にできるようになっています。ニュー・サン・ジョバンで新築される家屋では、小型の熱電発電システムが建築資材に内蔵されていて、太陽光の集光機能と家庭用蓄電池が備わっており、これらはすべて市のグリッドに接続されています。グリッドは社会事業として地元行政によって運営されており、Resila たち市民は地方税によってこれを支えています。その見返りとして、発電された電力は市内にのみ供給されます。

コネクテッドホームは成熟を迎えています。わずか 10 年前には、Resila は音声コマンドを使わなければならず、中央のハブに対してすべてのデバイスの設定を手動で行う必要がありました。今ではすべてのデバイスが互いに対話するようになり、環境の変化、仕事の予定、年中行事などに合わせて自動的に調整が行われます。コントローラでデバイスを調整する必要があるのは、設定を変更したいときだけです。不具合が起きるのはデバイスの 1 つが侵害されたときですが、ローカルやクラウド上の API によってデバイスに収集された情報が侵害されることが原因となるケースも増えています。昨年、Resila が友人をディナーに招いたと

きに、友人たちを家へ入れることができず、照明も点灯できなかったのは非常に決まりの悪い出来事でした。

Resilaの息子、Kojoは神経インプラントをしたいと母にしつこくせがんでいますが、Resilaは乗り気ではありません。Kojo の注意力はそもそも短時間しか続かず、それでなくても子どもたちはレンズ越しに注意散漫になるようなことに常に取り囲まれています。しかしKojo は、祖母がインプラント施術を受けたという友人を知っています。インプラントは、パーキンソン病の症状を緩和し、内臓やその他の生体サインを監視するほか、彼女が転倒した可能性がある場合には GPS と加速度計を使ってその時刻と場所を特定し、外傷を受けた強さと方向を記録して、必要な場合は救急車を呼びます。さらに、義手やその他の接続したいものを何でもコントロールできるようになりました。これが Kojo の目には最高に格好いいものに映るのです。医学的に必要であることと、ただ遊びのために欲しいというのは全然違うことだと、Resila は何度となく言い聞かせようとしました。しかし Kojo は根っからのゲーム好きです。体感が可能になった現在では、若者たちの間で「本当にそこにいる」と感じられることは特別な意味を持つようになったのです。ゲームの風景内にいることを体感するには、さらに素早い反応が求められます。インプラント手術をした Kojo の友人たちは思いのままの速さでゲームを操るようになり、Kojo は彼らに勝てなくなると危機感を募らせています。

学習時間中、子どもたちはレンズの学校レイヤのみをアクティブにしておくことになっていますが、Resila がどれだけペアレンタルコントロールを徹底しようとしても、Kojo 必ずといっていいほど回避してしまいます。レイヤが混ざると、センサーが収集する行動データも混合することになるので、Kojo が授業中に注意が散漫になり始めると詐欺師の標的になり、集中しているように見せかける覚せい剤や精神刺激薬の広告が表示されます。学校レイヤのみをオンにしているときでも、やはりハッカーはシステムを破って侵入し、見たくもない広告を表示してきます。Kojo の学校では、敬意ある態度とパーソナルスペースについて授業で教えていますが、ルールを守らず他者を傷つける子どもは必ずいるものです。どの年代の人も、自分の目で見たものを疑わなければならないことには難しさを感じています。

世界中の情報にすぐにアクセスできるようになり、物事を学ぶ必要性がなくなったため、現在の教育は知識の獲得よりも処理に重点を置いています。この結果として、人々が物事を客観的に捉えない傾向が強まりました。Kojo と Resila の目に見えるものは、アルゴリズムによって決定されます。アルゴリズム最適化は、文字どおり心と精神をめぐる闘いにおける重要なテクノロジとなっています。今や検索結果は主観的な真実であり、偽情報やプロパガンダを流布しようとする者は、その真実の操作を狙っています。インプラントが一般化するにつれて、人々の信条を効率的かつ直接的に操作することが、悪意の有無に関わらず可能になってきました。国連では、過去から現在に至るまでの歴史的事実の客観的記録を構築するプ

ロジェクトが進行しており、世界各国の政府が資金を提供しています。当然かもしれませんが、一部の国からは事実について合意を得ることが困難であることが、驚くほど多くの問題において判明しています。

Resila はすでに、自分自身の行動の変化に気づいています。携帯電話やラップトップの画面を眺めているとき、以前なら衝撃的な投稿やニュース記事を見かけても自分をそこから切り離すことができていました。一歩引いて時間を置き、ファクトチェックを行うことができました。しかし今では、高度にパーソナライズされた記事が、彼女の視界に直接送られてきます。レンズの文字数の制限により、主要なニュースは実質的にクリックベイトとなり、感情に訴え、目をそらせないことにより心理的な影響をもたらすものとなっています。視聴者がますます話にのめり込みやすくなっていることは、詐欺師や印象操作を狙う者がつけ込む機会になります。

Resila が 20 年前に最初の職に就いたときと比べれば、仕事の世界も様変わりしました。大パンデミックの時代に導入された新しい勤務形態は、多くの人々が在宅で何の支障もなく働けることを証明しました。Web 会議があまりにドライで味気なく感じられてくると、仮想現実や拡張現実が導入され、従業員が求めていた没入感と現実感のあるリモートワークスペースと、リアルなテレプレゼンスが実現しました。3D ビジュアルオーバーレイ、ジェスチャの取り込み、行動生産性メトリックが標準となり、Resila はどこにいても働くことができるようになりました。彼女の勤務先、KoRLo Industries が実際に運営するオフィススペースは全世界に 1 箇所だけで、別の国にあります。

Resila は近場への移動には自転車を使い、面倒なときにはタクシーポッドを使うこともあります。子どもたちも自転車に乗れる年齢になり、新しい個人用高速移動ポッドも使えるようになった頃、自動車税と保険の更新をやめることにし、車はガレージにしまわれたままです。高齢者や地方在住者はまだ車を持っています。化石燃料への禁止的な課税が開始されて以来、電気自動車が大多数を占めるようになっています。2030 年現在、ガソリン車、ディーゼル車、ハイブリッド車はいずれも新車販売されておらず、ガソリンスタンドは少なくなっています。

初めの頃は Resila も、運転手のいないタクシーポッドには奇妙な感じを受けました。しかしスマート道路での暮らしに慣れた彼女にとってはタクシーポッドは難しいものではなく、すぐに慣れました。彼女の両親にはもう少し説得が必要でした。今でも時々、父親がトラベルチップを忘れたり、反対方面に行ってしまったりといったときに、Resila に電話がかかってきます。街の中心部では車の使用は禁じられており、道路はドライバレス車両、e バイク、キックボード、そして自転車のための専用レーンで占められています。

ニュー・サン・ジョバンのダウンタウンも Resila が子どもの頃とは大きく変わりました。当時の街は、平日にはオフィス勤務の人々がせわしなく行き交い、絶え間なく騒音が聞こえる一方で、週末にはがらんとしていました。テレワークの拡大により、企業は高い賃貸料を払ってオフィスを構えるのをやめるようになりました。ダウンタウンが空洞化し、「ブライトフライト（有能な人材の流出）」といわれる人材不足の可能性にも直面して、市では郊外のショッピングモールを犠牲にして都市部の刷新を行いました。住居、娯楽施設、社交、またはクリエイティブな用途での物件賃料は大幅に引き下げられ、今では活気のあるレジャーハブとなっています。これは「リセントリフィケーション（再一極集中化）」と呼ばれ、中心市街地に人が再び集まり始めると、郊外に無秩序に広がっていた住宅街が縮小し、寂れた地域やゴーストタウンが残されます。

Resila は子どもたちを街へ連れ出し、テニスをしたりコーヒーを飲んだりするのが好きです。若者が多く住む都市部に比べると、ここではまだ小売店をいくらか見ることができます。高齢の人々は、人と接しながら買い物をし、買う前に実際に品物を見ることを好むからです。2、3 年前、Resila は市議会議員に当選しました。Resila は変わりゆく世界に適応できるこの故郷の街を、とても誇りに思っています。

デジタル版の個人というものが非常に広範なものになり、専門的な管理が必要になっています。Resila は、自分のデータを必要とするすべてのサービスに、プライバシー設定をブロードキャストするツールを使っています。このツールは状況に応じて許可を付与し、データには準同型暗号化が施され、Resila のみがアクセスできます。新たなサービスが彼女のデータを必要とする場合には、設定された規則に基づき、法的規制に準拠して、必要な情報へのアクセスだけが許可されます。

同時に、人間はユーザ生成コンテンツを通じて自身の生活の大部分を自発的に公開するようになったため、個人のアーカイブが必要になっただけでなく、そのアーカイブにより、本人が肉体的に死を迎えた後もデジタルな自己が生き続けるという状況が発生しています。かつてはソーシャルメディアでの思い出の集まりだったものが、今や生きた人間のように振る舞っています。ソーシャルスペースでやり取りを続けることで、残された遺族は癒されます。こうした「永遠の自己」の第 1 世代は、本人が生きていた頃に入力されたデータに基づいて、限られた一連のやり取りを繰り返す傾向にありましたが、最新のものは自己学習型で、最も親密な仲間や共通の趣味を持つグループの実際の人間に混ざって、新しい体験に関与できます。これらのデジタル人間は徐々に自我を持つようになっており、フィジカルとデジタルの世界が融合するにつれて特にその傾向が強まっています。彼らは不適切な行動に関与し、ときにはヘイトスピーチのような罪を犯します。政府当局は現在、デジタル人間が罪に問われるべきか、また彼らの不法行為に対してどのような法執行手段が適切なのかを検討していま

す。一方で、悲しみに暮れる遺族は、愛する人のスイッチが切られないように、また場合によっては法的強制力をもってスイッチを切るために、人権弁護士の支援を求めています。

b. ビジネス – KoRLo Industries

Konsolidated Rubber and Logistics (KoRLo) Industries は、創業 200 年の歴史を持つ重工業メーカーです。前世紀後半に天然ゴム製品から合成ゴム製品に事業展開した KoRLo は、タイヤ、テクニカル衣料品、ケーブル製造など、数多くの分野で世界的なリーダーになりました。医療用手袋の生産とウェアラブルデバイスへの事業展開によって、大パンデミック時代にはヘルスケア用品の分野にも進出しました。一方、自己修復ポリマーの合成への取り組みにより、同社製品は潜水艦用の通信ケーブルや急増する低軌道衛星にも利用されるようになりました。これらの製品だけでも、KoRLo は重要インフラストラクチャのサプライヤとしての役割を果たしています。

KoRLo の製品の多くは 2 つの目的で用いられるセンサーが搭載されるようになっています。エンドユーザの動作環境で使用される場合には、たとえばブーツの靴底やタイヤの溝の摩耗を分析して報告し、修理や交換が必要になれば所有者に警告します。宇宙や海底では、ポリマーシールやケーブルの絶縁に近く不具合が生じそうなことを予測します。これらのセンサーは、動作環境における壊滅的な障害の正確な診断情報を提供し、気象通報に貢献しています。企業として社会的責任を果たす取り組みの一環として、同社は主要な海洋浄化活動の後援とコンポーネントの提供も行っており、海底を浄化するためにケーブル絶縁材でマイクロプラスチックを吸引する方法を探る研究プログラムを指揮しています。

ポリマーに自己修復性がない場合や、何らかの理由で自己修復性が低下している場合には、インフラストラクチャ所有者が完全自律型の海中修理車両を展開できます。これらの車両は、ケーブルを全長にわたって継続的にパトロールし、海底の状態に関するデータを収集することもできます。現在では、KoRLo の原材料の大部分を再生プラスチック粒子が占めるようになり、同社は最近、国際合意で定められた画期的な目標である 80%のプラスチック再生率を達成しました。さらに、このモデルによって、KoRLo は生産拠点を海港や宇宙港に近い場所に移転し、輸送コストと環境への影響をさらに削減することが可能になりました。土壌汚染により古くから手つかずの産業施設の再利用は、同社の循環戦略の主要な部分です。

サプライチェーンと生産ラインの監視は、現在は完全にデジタルで行われています。AI と分析の進歩により、ほとんどの場合に物理アイテムとデータのセルフルーティングと自己修復が行われます。予測／予防保守はもちろん、KoRLo のカスタマーサービス、調達、運用の統合により、顧客から注文があるたびに自動在庫チェックが開始され、必要に応じて前駆化学物質やその他のコンポーネントの再発注が行われ、同社の半自律型貨物車両や、増加傾

向にある貨物輸送ハイパーループにも発送指示が出されます。その結果、効率とスピードの向上、ダウンタイムの短縮、リソースコストの削減が実現しています。このように自動化、自己修復、自律型ロジスティクスが発展した結果、機密性と可用性よりも、システム、データ、プロセスを優先するセキュリティテクノロジへの注目が高まっています。多くのユースケースにおいて、プロセスを破損または機能低下の状態で稼働させ続けるよりも、完全に停止することが推奨されるようになっています。

KoRLo は自社の IT インフラストラクチャを一切所有・運用していません。監視、保守、運用はすべてクラウドで行われており、すべての工場がスマート化され、サービスとして提供されているプラットフォームによって接続されています。新しい生産や既存の運用に対する変更が提案されると、これらは稼働環境に展開される前に同社のデジタルツインでテストされます。KoRLo は形状を変化させるようにプログラムされた製品を生産しているので、同社の DevOps は工業的、物理的な性質を帯び、ハードウェアと化学物質の設計と結び付いています。同社の従業員はこのハイブリッドプロセスを DesOps と呼んでいますが、世界の一部地域では、MakeOps という用語が一般的になっています。この完全にアウトソーシングされたインフラストラクチャを導入する際には、かなりの難題が生じました。KoRLo は、単純なユーザ構成を管理するのではなく、ユーザプロファイルの急激な増加を特定して、それに対処しなければならなくなっています。デバイスにはそれぞれに攻撃対象領域があり、その継続的な特定および評価も必要です。同社の専有データと PII データはこれまで以上に多くのシステムが格納先、アクセス元となっており、通過するソフトウェアインタフェースも多数に上ります。

KoRLo の人間の従業員は、自動化された作業のチェック、重大度の高い異常の調査と対応、ビジネス戦略の策定という、3 つの中心的活動に携わっています。Resila は、これらのうちの最後を担当しています。設計戦略チームのリーダーとして、彼女は同社の 4D プリント機能の買収に貢献しました。これは、GPS の刺激で形状を変化させることができる、宇宙輸送に適したフラットパック資材の生産に KoRLo が移行する決め手となりました。付加製造も、同社が医療分野、特にバイオエンジニアリングに進出する後押しとなりました。最近の Medist8 との提携による、自己折りたたみ式ポリマーステントの生産は前途有望でした。開発の次の段階は、プログラム可能なプリント細胞組織への新展開です。

Resila の役割は大きく変化しました。20 年前にこの仕事を始めたときは、コンピュータを使って通信機能のない製品を設計していました。セキュリティに関する最も大きな心配事は、競合他社や国家による設計の盗用に関することでした。その後 IoT の時代が到来し、アクチュエータやセンサーが非常に多くの製品設計に導入されるようになりました。KoRLo の市場には現在も異なる基準を採用しているところもありますが、大きな注目を集めた攻撃や訴訟によって、事実上の国際的な限界点とリスク選好度が定まりました。数年前、家庭用バッ

テリーの過熱事例が発生するようになり、家電用オペレーティングシステムに対する国家の関与による組織的なセキュリティ侵害が疑われた際には大パニックが起こりました。一部のバッテリーは爆発したり発火したりしました。被害を受けた顧客は現在、精神的苦痛と身体的傷害の補償を求めてメーカーを訴えています。

知的財産の盗難も、当然ながら依然として心配されます。単純なデータ搾取のほかに、KoRLo のようなメーカーはデータポイズニング攻撃を防ぐ必要もあります。盗難に遭った設計には、活発な闇市場が存在します。犯罪者は、最終製品が正しく動作しないように設計の構成を改変する手段も開発しました。オープンソースのテンプレートは、ポイズニングに対して特に脆弱であることがわかっています。最も小さな被害で済めば、影響として生じるのはダウンタイムと、最適な機能を発揮できないことに伴うコストです。医療と軍事の分野で機密性の高い事業を請け負っている同社の状況では、いくぶん大きな被害を受けることになります。不正なデータとプロセスの操作が、身体的危害を引き起こす可能性があります。

さらに、設計プロセスの大部分が自動化されている現在では、機械学習アルゴリズム自体、あるいはツールが学習に使用するデータプールのポイズニングが起これば、やはり予測できない結果が生じたり、最終製品の不具合や安全性の問題が発生したりする可能性があります。これを実行する能力があることを立証した犯罪者もいますが、多くのケースでは脅威だけで利益を生み出しています。現在でも脅迫が一般的な戦術であり、かつてのランサムウェアが証明したように、人々、企業およびその保険会社にはたいてい支払いの用意があります。サービス拒否攻撃やその他の形態の不正な攻撃や妨害は、設計段階でも、生産中、配送中、末端での使用中のいずれの時点でも起こり得ます。これらのすべてに対して、KoRLo はある程度までの責任を負います。

今から数年前、同社の消費者向け製品の利用者が盗聴の被害を受ける可能性があることに大きな関心が集まりました。センサーの数が大幅に増えたことでデータポイントの数も大幅に増え、個人の振る舞いや移動を測定し、推定するために使用されることになります。KoRLo のハイキング用ブーツに組み込まれたセンサーからのデータを使用した研究では、靴底の摩耗によって示される活動レベルと不安感の間に関連性があることが示唆されました。プライバシー擁護派と精神衛生保護団体は、同社がこの医療用ウェアラブルデバイスから報告された情報のデータを集約していること、また法執行機関などの政府当局がデータに自由にアクセスできることを懸念しています。さらに同社が医療機関と保険業界にテレメトリを提供することにより、このデータから金銭的利益を得る手段を検討しているという噂も広まっています。

こうしたことは、陰謀論者の怒りをあおる恰好の材料になっています。当然のごとく彼らの関心は、かつてのワクチンや電話用の電波塔から、彼らが体内監視技術と考えるナノメディ

シン、バイオエンジニアリング、コネクテッドインプラントといったものに移っています。KoRLo もこうした陰謀論に巻き込まれており、いかに正確さを欠いた考えであれ、暴力的な脅迫を常に受けています。同社の広報部門には現在、ファクトチェックと陰謀論の反証を専門とするチームがあります。競合他社の施設では数年前に発砲事件が起こり、KoRLo の自社システムに対しても自動化された大規模な分散サービス拒否攻撃の試みが頻繁に確認されていることから、これらは中身のない脅しではないことがわかります。ボットネットも進化を遂げており、侵害された IoT を利用すれば、同社自身の大規模に接続されたデバイスを悪用して、内部 DoS 攻撃を仕掛けることが可能になっています。

このような理由から、従業員の調査をさらに強化することがますます重要になっています。インサイダーによる脅威が常に問題になっており、KoRLo は高度なアクセス制御と ID 管理ツールを幅広く使用していますが、不正アクセス、妨害、データ搾取の発見はますます複雑な作業になっています。同社の職員の多くは、オフィスや工場に足を踏み入れることがほとんどありません。社内の業務で使用されたり、生産されたりしている、数百万台のデバイスが生成するデジタルノイズは相当なものです。これらのデバイスは企業インフラストラクチャ上には存在せず、5G 接続に依存しており、処理はパブリッククラウド内で分散エッジコンピューティングによって実行されます。

自動化された攻撃の頻度、量、スピードにより、KoRLo は自動化されたインテリジェントな防御に重点的に投資する必要に迫られました。かつてビジネスメール詐欺と呼ばれていた攻撃は、人間による誤りがなくても成功するようになりました。完全に自動化されたサプライチェーンでは、人間による許可がなくても請求書の支払いが行われます。

これに代わり、ビジネスプロセス詐欺が台頭してきました。KoRLo などの大企業では、プロセスの異常を防止および特定するために分散台帳（ブロックチェーン）テクノロジを利用しています。現在、Tier 1 セキュリティ運用タスクは完全に自動化されており、人間は人工知能によってトリアージとエスカレーションが行われたケースのみに対応します。

人間の従業員のために拡張現実を導入した没入型インタフェースの採用が進んでいることも、自動化された防御が重視されるようになった要因です。レンズとスマート仮想ルームが導入されるや否や、フィッシングの試みが成功することが増えました。従業員は視線のすぐ先で、あるいは没入している世界の中で行われる詐欺の方が無視することが難しく、騙される可能性が高くなるということに世界中の企業はやがて気づきました。また、仕事中の不快な体験に動揺する度合いも大きくなりました。Zoom 爆撃は、大パンデミック時代に勢力を増した初期のビデオ会議テクノロジにちなんで名付けられた現象ですが、環境の没入性の向上に伴って進化を遂げました。こうしたことから、従業員の間ではセキュリティ意識向上プログラムへの関心がますます強くなりました。セキュリティインシデントが技術的に複雑化してい

るにもかかわらず、人間による防御はまだ全廃に至っていません。現在の課題は、敵対的生成ネットワーク（GAN）によって動かされる、現実そっくりにデジタル化された同僚と日常的にやり取りする環境で、疑わしい活動や虚偽の活動を識別できるよう従業員をトレーニングし、従業員がこうした活動を報告し、無視するための適切なツールを状況に応じて提供するにはどうすればよいかということです。

一方、KoRLo の人間以外の作業員は、これまでと変わらない生産性を維持して、同社の利益を支えています。このため、「悪党ロボット」シナリオのリスクを最小化し、ネガティブな体験の入力が最小限になるように運用環境のチューニングを常に維持することが、セキュリティチームの要点になっています。しかし、これだけ多数のエンドポイントと多数の API が多種多様なネットワーク上にある状況では、対策は時間との闘いです。

c. 行政 – ニュー・サン・ジョバン

ニュー・サン・ジョバン市（NSJ）はテクノロジ導入の最先端を行く都市です。数多くの大手テクノロジ企業の本社が市内や近郊にあり、たびたび新興テクノロジの実験の場となっています。また、NSJ の住民のプライバシー意識は世界で最も高い水準にあります。数年前、この国の政府は、国民全員に単一のデジタル ID を付与することの是非について問う、異例の国民投票に踏み切りました。NSJ は国内最高の投票率を記録しただけでなく、市民は旅行、健康、税、雇用、教育に関するデータの集約に対して 73%の大差で反対票を投じました。全国的には接戦の結果になり、52%が反対、48%が賛成でした。

この国民投票に法的な拘束力はありませんでしたが、その結果は民意として、当面受け入れられました。政府は、国民全員が単一のデジタル ID を持つことは、効率とセキュリティの向上をもたらすと主張しています。プライバシー擁護派は当然、ユビキタス監視と、クロスプロファイリングによって不公平な処遇を受ける可能性について懸念しています。

隣国の東サン・ジョバンでは、独裁政権によって「望ましくない」とされた人々が教職に就くことは、若者を堕落させるという恐れから禁止されています。税金を滞納している国民は、公共医療機関を利用することができません。

ニュー・サン・ジョバンの市議会では、循環経済における良い行いを奨励するために、データの集約を拡大しようという動きがあります。すでに、定められたとおりにリサイクルを行っていることがスマートゴミ箱によって記録された家庭は、公共交通機関を割引料金で利用できます。ペダル式自転車と e バイクに乗る「責任意識と敬意が高い」と認められた人々は、繁華街のソーシャルゾーンで飲食物の割引を受けられます。

セキュリティ専門家の意見によれば、異なるデータセットを結合することはテロリストや犯罪者の追跡に役立つ可能性がある一方で、ハッカーや印象操作を企む者にも大きな利益をもたらします。注目すべき 2 種類の反応が起こっています。セキュリティツールを使用して、自分たちのデータセットを隔離された状態に保とうとする市民の数が世界中で増加しており、その多くはデジタルデータ収集そのものに抵抗しています。この人々は「スプリッター」と呼ばれるようになり、環境活動家やオフグリッド生活者と同調する傾向にあります。NSJ はスマートシティであり、オフグリッド生活は実質的に不可能なので、市境から約 20 km 離れた田園地帯に新興の代替コミュニティが拡大しています。同時に、単一デジタル ID のメリットを支持する一部の市民は、より強力な法律の制定と、政府による監視と差別化されたプライバシーに関連する透明性の向上を提言しています。ここ数年は後者が優勢になっており、たとえば医療提供に関するビッグデータ分析において、実際のアイデンティティをさらす場面を減らしつつ（完全に不要になったわけではありませんが）、そのメリットを実現しています。

使い捨てプラスチックは NSJ では完全に禁止され、あらゆる形態のプラスチックが段階的に廃止されています。化石燃料由来の製品も法律で禁止されているので、地元メーカー（KoRLo の競合他社を含む）はバイオプラスチック生産への転換に苦労しています。その企業の 1 つ、Compfabrik は地域の産業用高温堆肥化施設に出資しており、この施設では廃棄バイオプラスチックを利用して市のために熱と電力を生成しています。

10 年前、外国製通信インフラストラクチャ用コンポーネントの輸入制裁措置によって、5G テクノロジの導入が多くの国で遅れました。この国の政府は国内通信会社の製造事業を復興させ、6G の立ち上げに必要な材料と機器の研究プログラムに注力しました。この国は、同盟国に対する 6G テクノロジとコンポーネントの主要サプライヤになろうとしていますが、国家間でのテクノロジの不均衡が今はかつてないほど大きくなっています。

ニュー・サン・ジョバンでの 5G の大規模展開は、「友好国」の企業からのコンポーネント供給によって実現しました。これによって、このスマートシティでの主なイノベーションのいくつかが可能になりました。たとえば、接続は個々の市民にシームレスに提供され、拡張現実の映像と投影を外出時にも切れ目なく見ることができ、交通網は世界で最も高度な技術を導入しています。

自動運転車テクノロジで世界最先端の企業が近隣にあることが契機となり、新興住宅街のジオフェンス地域内で、半自律走行のタクシーポッド専用レーンが市議会によって指定されました。ダウンタウンではガソリン車は走行しなくなりました。市の全域ではまだ何千台ものガソリン車とハイブリッド車が登録されているため、完全な禁止には至りませんでした。今

年の初めに燃料税が大幅に増税されたことで、すでに消費者の行動は変化しており、市議会のイノベーション資金にもなっています。

NSJ は完全なキャッシュレス社会です。高齢者はまだデビットカードとクレジットカードを使っていますが、ほかの年齢層での利用は大幅に減少しています。国の不換通貨と結び付いたデジタル通貨が幅広く使われ、顔認証による決済の確定など、幅広いバイオメトリック機能が付加されています。ただし、デジタル通貨には匿名性がないため、プライバシー意識の高い層にも犯罪者にも敬遠されています。現金が一般にあまり利用されなくなると、公然と現金を使い続けていた犯罪者は即座に特定されました。現在、犯罪者は現金を暗号通貨と交換しやすい外国に運び出すようになっています。

Resila は希望して市議会のセキュリティ担当の職務に就いており、その一環として警察や国のサイバーセキュリティサービスと連携しています。国家レベルでは、法執行機関と諜報機関が外国の攻撃者による印象操作、特に民主的プロセスへの干渉に頭を悩ませています。政治家の音声や映像の偽造や改変を識別するためのソリューションは開発済みですが、エンターテインメント業界や正当な政治運動でも合成の音声や映像が幅広く利用されているため、ソリューションの効果的な活用が難しくなっています。市民は AI によって生成される映像に鈍感になっています。今や、AI 生成の映像はきわめて正確で実物そっくりになっているので、合成コンテンツと本物のコンテンツの区別が付けられません。同時に、こうした映像が市民の目の前で提示されると、無視することは難しくなり、より信頼できるように見え、より直接的に感情に働きかけてきます。かつて、印象操作の実際の影響について懐疑的だった人々も、その流れを汲んだ技術の高い効果を目の当たりにすることになりました。偽情報は、人工的に生成されたアバターとの本格的な没入型の会話へと進化し、市民の考えや企業の方針さえも変えられるものとなりました。

テクノナショナリズムの影響は、通信インフラストラクチャのみにとどまりません。侵害されたデジタルコンポーネントが関与する大規模な攻撃が注目を集めて以来、サプライチェーンは長年にわたって官民の両セクターで厳しく監視されてきました。規模の大きな企業は、調達先の選定の厳格化に伴うコスト増大をある程度は吸収できましたが、地方自治体では体制の再構築に時間がかかりました。また、こちらの点の方が重要かもしれませんが、NSJ 市議会のような行政機関の顧客は、民間企業ほど予算に余裕がありません。サプライチェーンのセキュリティの経験がある Resila は、市議会の監督を依頼されています。その中で気づいたのは、セキュリティに関していえば、予算の制約による影響を受けているのはサプライチェーンに限らないということでした。財務面での制約は、セキュリティのために利用できる人材面、技術面でのリソースにも決定的に影響します。NSJ のようなスマートシティでは、セキュリティを確保できなければ物理的な破壊と身体的な危害につながる可能性があります。特に、次世代ランサムウェアやデータポイズニング攻撃によってスマートシティの管理が拒

否されたり妨害されたりし、輸送、医療、教育、税務、物流などのサービスに使用される API が公開された場合は、甚大な被害が生じます。

Massive Internet of Things（MIoT）と 5G の時代には、あらゆるものが SIM 経由で接続されています。膨大な数のデバイスとセンサーの相互接続からは新しい種類の攻撃や昔ながらの攻撃のための新しいベクトルが生まれました。法執行機関はスマートシティにボットネットが到来することは予測できましたが、IoT 侵害が料金詐欺という手段で金銭的な被害をもたらす可能性は察知できませんでした。数カ月前、同市にある街灯の一部が、割増料金のかかる電話番号に電話をかけていたことが判明しました。国際警察の捜査により、数百万台の車両と家電も侵害を受け、電話回線の所有者が金銭的な利益を得ていたことがわかりました。

新しく設立された国際検察当局が起訴を目指していますが、犯罪者が潜んでいるとみられる国はこの機関に非加盟で、起訴への対応を拒否しているとも伝えられています。

IT の犯罪的悪用に対する国際的な取り組みによって、国家の関与しない攻撃者への多国間行動が可能になり、その審理は大きな関心を集めました。しかし、最も危険な犯罪者は今でも国家による支援を受けているという暗黙の了解があります。同様に、国家による攻撃的サイバー操作の適正使用に関する協定があるにもかかわらず犯罪グループによる攻撃はなくなっておらず、グループが国家と関係しているかの見極めはますます難しくなっています。各国政府は建前上は不法行為を非難する必要があるため、サイバー攻撃者の迅速な特定を一層困難にするツールの進化が促される結果になっています。サイバースペースでの適切な行動の規範と原則を制定しようとする多部門にわたる取り組みは、熱狂的に受け入れる向きもありますが、疑念の中心とする向きもあります。

NSJ の市境のすぐ外には、半自律型兵器の軍事施設があります。昨年、殺傷能力を持つドローン数機が、工場から基地に輸送される途中で盗まれました。まだ攻撃には使用されていないものの、外国のテロリストグループの手に渡った可能性があることが諜報機関によって示唆されています。NSJ の独立の機密情報収集／偵察部門が確認した情報によれば、攻撃者は地下ネットワークでドローンのアクティベーションキーを探していたことがわかりました。唯一の是正策は、関連する範囲内のキーをすべて無効化することでした。機密情報部門は現在、テロリストがキー生成プログラムを探していることを示す会話を特定する作業を進めています。ソフトウェア定義の一時ネットワーク（5/6G）が登場してからは特に、特定は難しくなっています。基地に収容されている自己学習ミサイルシステムのコードとトレーニングデータの変更が試みられたこともありました。

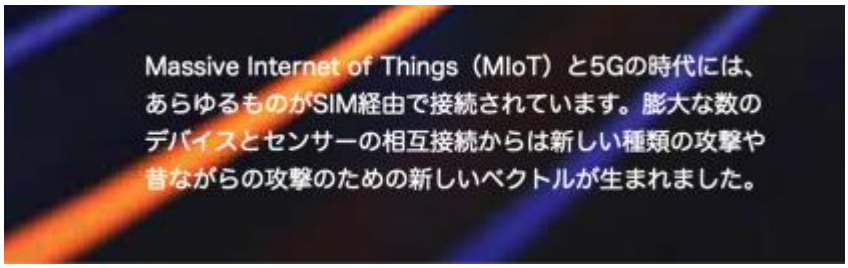
完全自律型の兵器システムについては、依然として国際的な議論の対象になっています。現在のところ、これらのシステムのテストは一時停止中です。ニュー・サン・ジョバンはその条件に従っていますが、国連安全保障理事会では東サン・ジョバンが違反行為をしていると

いう疑惑が持ち上がっています。地域での緊張が高まる中、ほかの国々は禁止措置への支持を撤回すると脅しをかけてきています。

ほとんどの地方自治体と同様に、NSJ の市議会は過去 30 年間に生成された膨大な量のデータの格納と管理に苦慮しています。地元のテクノロジ企業は、データを DNA に格納するソリューションの試用を市議会に持ちかけました。とりわけ保存できる情報に関してはこの技術によって大幅な効率改善が期待できますが、いかに人工的であろうとも生物学的素材をこのように利用することに、一部の市民は反対しています。宗教団体と陰謀論者は、それぞれ異なる理由で特に激しい主張を繰り広げています。

生体工学に基づく攻撃と、プログラム可能な素材に不正プログラムが仕込まれるという新しい傾向が明らかになる中、一般大衆は当然のことながら、身体的な安全に危害を及ぼす可能性があるサイバー脅威に神経を尖らせています。

量子処理に向けた進歩も急速なペースで続いており、2048 ビット RSA アルゴリズムの量子復号化も実現間近です。各地の自治体は、ポスト量子暗号への移行について数年にわたり警告を受けてきましたが、移行の実施時期と実施方法については標準化されておらず、ガイダンスも存在しないため混乱が起きており、サードパーティソリューションへの過剰な依存と、場合によっては過剰な支出が生じ、世界の一部地域では準備不足が問題になっています。情報が錯綜する中、Resila は NSJ の幸運を祈り続けており、幼い頃の 2000 年問題のように、心配が杞憂に終わることを願っています。



サイバー脅威

シナリオストーリーで描いた犯罪行為は、以下の一般的なカテゴリに分けることができます。

2020 年のケースと同様に、1 つのサイバー脅威ビジネスモデルが、これらの行為のいくつかに順次、または同時に関与する場合があります。たとえば、現在流行している二重の脅迫を行う標的型ランサムウェアは、データを搾取するための不正アクセスと、レバレッジとしてのサービス拒否攻撃を必要としますが、搾取したデータを公開するという脅しの形での二次的なレバレッジも必要とします。

この取り組みを前回実施したときの結果と同様に、上記の犯罪行為は少なからず、すでに明らかになっている脅威を進化させたものです。2030 年に至る過程で変わる点は、少なくともここで作成したシナリオストーリーから見えてくることでいえば、イネーブラ、標的、攻撃の潜在的な影響です。

今後 10 年間には、反復操作の自動化が以前にも増して進められるとともに、機械学習が高度に発展し、組織、社会のあらゆる分野で人工知能を搭載したツールが使われるようになることは確かです。この利用者には当然、個人、犯罪組織、国家などの攻撃者が含まれます。特に、高度に自動化された偵察、標的の選択、ペネトレーションテスト、実行はサイバー犯罪者にとって好都合であり、教師なし学習が可能なツールを使用して犯罪活動の有効性と効率を最大化しようとすることは、合理的に推定できます。CaaS（Crime as a Service）の犯罪市場について私たちがすでに把握している状況から考えれば、不法な AI 対応ツールの販売により、専門的な技術力のほとんどない個人でもサイバー犯罪の企てを実行できるようになると予想できます。これが火付け役となって、ハッカーというより運営者／管理者の性格が強いサイバー犯罪者が急増することが考えられます。

AI による攻撃は、より高度になった難読化技法によって支援されることは必至で、おそらく難読化自体が AI によって強化されるでしょう。データの取得と特定を逃れるための自己学習 Fast-Flux ツールは、既存のアノニマイザが論理的に進化したものです。しかし、AI によるサイバー防御にまつわる現在の議論で話題になっているように、「自動の」サイバー犯罪は、運用者がその動作について完全に理解していない場合、その意図しない中断の機会を生む可能性があります。

同様に、AI の正しい動作への干渉も、犯罪者に都合の良い機会をもたらすことが考えられます。AI の学習に使用されるデータセットの操作を伴う複雑な攻撃は、安全性の問題やロボットによる不正行為など、悪い結果を巧妙に作り出します。こうした方法は、知的財産の盗用よりも洗練された手段で競争優位性の獲得を狙う、十分な資金力のある企業や国家にとっては特に魅力的かもしれません。

同時に、これらのシナリオでは、データ操作が人々や物体に対してより直接的な影響を及ぼす可能性があることが強調されています。データが主な要素になる 2030 年のサプライチェーンでは、たとえば食料品の生産や医薬品の提供において、成分や指示が改変されると身体的危害につながる恐れがあります。このようなシナリオでは、サイバー攻撃を受けると実際の製品が回収される結果になります。脅迫者による悪用の範囲には、スーパーマーケットで販売されるベビーフードにガラス片を混ぜるような古典的な手口と大差ない手段も含まれるでしょう。一方、インプラントや人工装具によって人体がインターネットに物理的に接続するようになると、生理機能に妨害や損傷が引き起こされる可能性が出てきます。ブレインコンピュータインタフェース（BCI）の導入も同様に、神経学的プロセスの完全性に関する問題を引き起こします。不正アクセス、サービス拒否、搾取、ランサムウェアといった確立された脅威が、細胞組織に埋め込まれたセンサーに移行されるというだけで、その脅威を説明するに十分であり、一部の人々にとってはまさに死と同等の脅威になる可能性があります。

少し離れた場所にある画面とは異なり、没入型テクノロジとヘッドアップディスプレイ（HUD）によって情報がすぐ目の前に提供される世界では、データ操作が印象操作や偽情報に悪用されることが考えられます。今後、アルゴリズム最適化（SEO の後継技術）が反復されると、善意であれ悪意であれ、信念を変える力が高まっていく可能性があります。脅威ベクトルとしてのソーシャルエンジニアリングも同様に、体験の緊迫感によって反応を急がされ、批判的な視点を保てる距離が短縮された環境では、抵抗が難しくなるかもしれません。インターネットを媒介とするサービスによるマインドコントロールは、2020 年の時点ですでに目立つ存在になっていることは確かですが、シナリオで予想した 2030 年には情報の説得力がはるかに増しているでしょう。自然言語処理と GAN のさらなる進歩によって、より本物らしく、より人間らしく見えるように合成された、偽情報による詐欺が展開できるようになることも考えられます。

モノを狙った脅威は、MIoT という形で接続された標的を数十億規模で操れるようになります。処理能力のハイジャックが可能であることは、既存の IoT ボットネットがすでに実証しています。シナリオで予想した事例はさらに一歩進んで、MIoT 侵害から金銭的な利益を得ています。街灯が割増料金の番号に電話をかけるという考えは、一見少し奇抜に思えるかもしれませんが、すでに確立されている電話回線の登録と料金にまつわる詐欺の企てから着想を得ています。

真の MIoT 環境では、サイバー攻撃が成功すれば、製造や物流のみでなく、輸送、医療、教育、小売、さらに家庭環境でも混乱を引き起こします。付加製造、特に 4D プリントにおいては、センサーに対して妨害やサービス拒否が仕掛けられると、製品の形状や状態が意図したとおりに変化しなくなる可能性があります。

さらに、シナリオのストーリーで予想した 2030 年は、エッジ処理と分析によって製品の自己ルーティングと自己改変が促進される時代です。この未来では、アルゴリズムの自己学習と自律性も強化されるので、インサイダー脅威に対する私たちの認識も進歩が必要になるでしょう。これまでは組織に対する人間のリスクを指すものとして理解されてきましたが、2030 年のインサイダー脅威はオブジェクトやアルゴリズムであることも十分に考えられます。

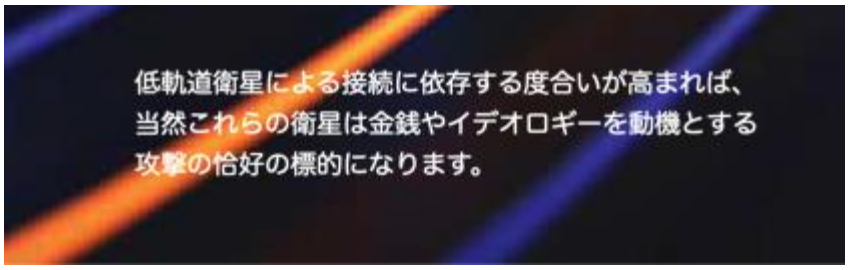
ニュー・サン・ジョバンでは、サードパーティやサプライチェーンに対する侵害が 2020 年よりさらに顕著になっています。EaaS（Everything as a Service）の世界では、巨大なクラウドベースのサービスプロバイダの侵害に成功すればさらに大きな収穫が得られ、1 つの企業ネットワークに不正アクセスするよりも確実に大きな影響力があります。一方、不正プログラムがプリインストールされた状態で出荷されるコンポーネントの現在の信号に相当するものは、シナリオのストーリーでは、影響を拡散させる感染物体として動作環境で描かれています。

接続された物体が海底や地球の周回軌道内にあれば、サイバー犯罪の影響がかつてなく広い範囲に達する可能性があります。5G および 6G によって、このきわめて膨大な数の接続と、IoT 導入の大幅な進歩が実現し、おそらくその影響が最も顕著に見られるのは都市環境でしょう。5G と 6G の幅広い受信可能範囲と、センサーの急増が複合的な要因となって、より壮大な規模でのサイバー脅威が現実のものになります。一方で、シナリオに描かれていたシームレスな接続により、位置情報に基づいて攻撃の標的をより効果的に絞り込むことが可能になり、都市または国全体の統合サービスやネットワークを停止させたり、乗っ取ったりする攻撃も起こり得ます。シナリオで予想されていた未来では、より広範囲でありながら、より特定された地域を狙った攻撃が、次世代ワイヤレステクノロジによって可能になっています。

低軌道衛星による接続に依存する度合いが高まれば、当然これらの衛星は金銭やイデオロギーを動機とする攻撃の恰好の標的になります。自動運転車の妨害やハイジャックに関心が集まっていることはすでに明らかになっており、この関心は今後 10 年間に強まっていくと見るのが妥当です。5G テクノロジへの疑念によってすでに実証されているとおり、新興テクノロジへの抵抗は物理的破壊という形で現れることがあります。このテクノロジが、データを収集して報告し、刺激に反応する製品の急増を招くだけでなく、AI の進化も促進する世界では、テクノロジの進歩を中断または遅延させることを目的とした、物理的な攻撃やサイバー攻撃が起こることが予想されます。地域によっては、個人データの収集と監視が強化されることへの不満が、治安の悪化を招く可能性もあります。

シナリオのストーリーで描かれた世界では、新しいグレーマーケットや犯罪小売市場が登場しています。勤務中の監視に対する抵抗は、従業員のリアルな視聴覚的表現を誇る企業向け生産性モニターを巧みに欺く、AI 搭載のツールの誕生を促すかもしれません。このような状況では、行政機関、企業、消費者の環境でもっともらしく別人になりすます能力により、ID 窃盗がさらに巧妙化することにもなりそうです。

幅広いサービスにまたがって一元化された国民 ID を採用している国では、認証情報が犯罪者にとって価値の高いものになります。デジタルツインのアクセス認証情報を入手すれば、犯罪者は組織のネットワークとサービスの高度な偵察を実行でき、不正な活動を開発段階でテストすることさえ可能になるかもしれません。一方、ウェアラブルデバイスやインプラントなど、センサーを内蔵した物体によって収集されるライフスタイルデータがさらに増加すれば、次世代の消費者監視ツールによって悪用されることは必至です。より巧妙なストーカーウェアによって、サイバー暴力が助長される可能性もあります。



シナリオのストーリーでは、新しい脅威ベクトルと犯罪手口についてスペースを割きましたが、従来のスタイルの攻撃が存続する余地も同じくらいあります。たとえば、実際の小売店舗が今後も存在し続ければ、PoS（Point of Sale）侵害の実行可能性も継続することになります。ニュー・サン・ジョバンの例で想定したように、このような活動の影響を受けるのは、高年齢層と先進テクノロジをあまり利用しない層に偏るでしょう。

サイバーセキュリティ利害関係者への影響

セクション 3 に示したシナリオは、考慮すべきいくつかの事項を今日の利害関係者と意思決定者に提起しています。考慮事項には以下が含まれますが、これらに限りません。

サイバーセキュリティのビジネスの変化

AI によるサイバー攻撃、防御、インシデント対応の未来では、人間の役割は高度化します。人間による検証にエスカレーションするためのしきい値は高くなるものの、データ保護と違反通知の要件を含む、法規制に関する考慮事項の影響も受けます。シナリオのストーリーに描かれていたように、セキュリティ専門家が集中的に取り組むのは、戦略とポリシーの設定、パフォーマンスの監視、および実施した措置の説明です。この最後のもののためには、AI 搭載のセキュリティツールが説明可能なものである必要があります。一方で、コアアクティビティの変化により、人間のスキルセットも変化することが予想されます。アンケート参加者の 1 人が述べていたように、「5 年以内に SOC（セキュリティ運用センター）のアナリストはデータサイエンティストになる」でしょう。

セキュリティと IT 運用がアウトソーシングに向かう傾向が継続することはアンケート参加者の評価とも一致しており、2030 年には「サイバーセキュリティの大部分は AI による攻撃と防御で占められるようになる。毎日がゼロデイになる」（Q.12）という設問には 63%、「データを管理する人間が気づく前に AI が侵害を当局に報告する」（Q.20）という設問には 66%が、起こり得ると回答しています。AI サイバー攻撃は高速で実行されるため、自己学習機能を搭載した難読化ツールによって特定作業が妨害されるような場合には特に、迅速な特定が困難になります。攻撃者の特定がほぼ実行不可能なシナリオでは、攻撃者に対する法執行の取り組みが、一方では注意が足らず技術水準の低い攻撃者を追跡すること、もう一方では国家による支援を受けている証拠がある攻撃の調査にリソースをつぎ込むことに限定される危険性があります。国家による支援を受けているグループは、次世代の犯罪的セキュリティツールを利用するためのリソースを持っている可能性が高いので、捜査当局と犯罪者の知恵比べという、すでにおなじみのツールと技術開発の競争が今後も展開されることになるでしょう。

より一般的なレベルでは、AI による攻撃／防御モデルの登場により、必然的に法執行よりも予防とインシデント対応の活動の方が重視されるようになります。AI によるサイバー攻撃が使用する戦術、技法、手順（Tactics, Techniques and Procedures、TTP）は、すでに人間による攻撃で考案され、利用されてきた方法論に必ずしも限定されません。私たちは、新手の攻撃方法に関する実験と調査を長期間にわたって続けることになるでしょう。この状況では、技術面と人的な面のどちらでも、脅威インテリジェンスの価値がさらに高まります。

さらに、以前の Project 2020 ホワイトペーパーでも提起した問いですが、さまざまなサイバーセキュリティ利害関係者の役割と責任について考え直す必要があります。たとえば、攻撃の特定による法執行の可能性がさらに低下している世界では、法執行要員は活動の妨害と人的諜報活動の展開を目的とした、犯罪グループへの潜入に再び集中的に取り組むようになるかもしれません。

境界の死：エッジでのセキュリティと ID

何十億ものオブジェクトが 5G および 6G に接続され（MIoT）、エッジでの処理と分析、真の分散／クラウドコンピューティング、EaaS（Everything as a Service）が実現する未来では、サイバーセキュリティが歴史的に固執してきた、境界とネットワークに基づく保護からの脱却が求められます。コンピューティングとセキュリティのパラダイムは、2020 年のかつてなく急速なリモートワークへの移行に促されて、すでにこの新しい要件を満たすべく進化しています。SD-WAN（Software-defined Wide Area Network）、SWG（Secure Web Gateway）、CASB（Cloud Access Security Brokerage）、FWaaS（Firewall as a Service）を含む、SASE（Secure Access Service Edge）という概念の人気が高まっていることは、物理ネットワークのセキュリティモデルが近いうちに陳腐化するという認識の表れです。一方、ゼロトラストのアプローチは、組織のセキュリティに境界がますます無関係になっているという認識に沿ったものです。

したがって、IAM（Identity and Access Management）への注目が高まっているのは情報セキュリティ機能のための当然の動きです。シナリオのストーリーの世界に描かれているのは、さまざまなデバイスとサービスにわたるデジタルアイデンティティの高度な統合、オフラインの人間やデバイスと一致しない合成アイデンティティ、さらに人間が状況に応じてアイデンティティを改変する機会のさらなる増加です。このような未来でセキュリティソリューションが効果を発揮するには、このような複雑性の認識とそれに対する備えが必要です。

統合されたサイバーセキュリティ

没入型テクノロジがニュー・サン・ジョバンで見られるほど高度に導入されると、ヘッドアップディスプレイによる認証（たとえば、虹彩認識による）が人間の認証手段としてさらに広く普及するようになると考えられます。没入型テクノロジによってもたらされる脅威とサイバー暴力の心理面、感情面での潜在的な影響により、未来の情報セキュリティ要員は、緊急対応時にメンタルヘルスの専門家と緊密に連携することになるかもしれません。また、攻撃を受けた体験に関するデータを分析し、提示するよう求められることも考えられます。IT 詐欺や不適切なコンテンツの提供が原因で心理的危害や精神的苦痛を被ったとする訴訟が起こされる可能性も排除できません。同様に、情報セキュリティの専門家は、接続された医療

デバイスが関与する傷害や死亡について調査するように求められるでしょう。検死解剖の過程ではデジタル証拠が常に精査され、検死法廷では CISO が証言を求められるかもしれません。アンケート参加者の 1 人が指摘したように、サイバーフィジカルセキュリティは重要インフラストラクチャのみに適用されるものではなくなります。「OT（運用テクノロジ）と制御システムに見られるサイバーフィジカルリスクが、あらゆる場所で生じるようになるでしょう。身体や環境への危害を引き起こすサイバー攻撃は、月並みなデータ侵害の影響を大きく上回る被害をもたらします。失われるのはデータではなく人間なのです……」[3]

一方、シナリオのストーリーでは、インターネットに身体的に接続されることに乗り気でない人々も社会には出てくると推測しています。現在も、5G や新型コロナウイルスのワクチンなどの進歩に対して一部の層から疑念が生じており、中でもワクチンに無料の追跡マイクロチップが仕込まれているという陰謀論がおそらく最も顕著に示しているように、テクノロジは身体的危害と容易に関連付けられることがあります。医療でのユースケース以外でも、身体にデジタル拡張を施す可能性について若年層があまり恐れていないニュー・サン・ジョバンと同じように、世代間の分断が生じる可能性があります。このことからサイバーセキュリティのコミュニティが推測できるのは、若年層の標的グループと、医療面で脆弱な人々の侵害リスクが高まることです。

すべてがサイバー化した現在

2012 年の Project 2020 のシナリオではすでに、サイバーセキュリティと国家安全保障の間には重なる部分があり、サイバーセキュリティと国際関係の間に複雑な相互作用が生じることを予想していました。現在の報告は、国家による、また国家の支援によるサイバー脅威活動の性質の変化を反映しています。一方で、国や地域はデジタル主権の維持をますます重視するようになっており、世界最大の勢力を持つ国のいくつかではテクノナショナリズムが重要な戦略地政学的手段になっています。シナリオのストーリーが示しているように、サプライチェーンに制約があると新興テクノロジの導入が遅れるだけでなく、テクノロジを保護する能力にも影響が及びます。サイバーセキュリティにおける国産のイノベーションを推進しようと今から行動している国は、外国のサプライヤに依存する国よりも、この予想される未来の難題をうまく切り抜けられるでしょう。

こうした未来では、情報セキュリティ専門家は調達対象の選択についてさらに厳しい精査を受けることが予想でき、以前よりも可能な選択肢が少なくなることも考えられます。さらに、サイバースペースのガバナンス（主権地域とサイバー運用の規則を定めること）と、インタ

[3] Q.35：「情報セキュリティ専門家が夜も眠れなくなるほど心配することは何でしょうか？」に対する自由テキストの回答

ーネットのガバナンス（コンテンツの規制）の区別はさらに曖昧になり、多面的な明確化が行われなければ完全に消滅する危険もあります。テクノナショナリズムとデジタル主権の傾向がますます強まっていけば、真にオープンな市場に小さからぬ難題をもたらすほか、真にグローバルなインターネットの可能性を永久に閉ざすことになります。

テクノロジの不均衡

本書で述べているシナリオは、新興テクノロジが最大限に導入されてきた社会を反映するよう、意図的に構築されたものです。ニュー・サン・ジョバンに国際的なパイオニアとしての特徴を設定したのは、広範囲のテクノロジの応用とサイバー脅威について検討するために十分な余地を設けるためでした。シナリオのストーリーで述べた先端技術が世界のすべての地域で同程度に利用できると想定することは、きわめて非現実的です。それどころか、アンケート参加者のほぼ半数は、インターネット接続が今後 10 年以内に世界の全人口に普及することについてさえ、悲観的な見方を示しています。量子コンピューティングのような画期的な可能性を秘めたテクノロジも同様に、突如としてだれもが利用できるようにはならないでしょう。

世界最大級のテクノロジ企業と、潤沢なリソースを利用できる研究機関がこの分野のパイオニアであり、量子処理をサービスとしてリースする準備をしています。したがって、量子処理能力のバランスは比較的少数の地域に偏り、購入資金があるユーザにはサービスが少しずつ提供され、テクノロジにおける「持てる者」と「持たざる者」の不均衡はさらに拡大していく可能性があります。こうした不均衡の影響は、2020 年の時点ですでに認められているサイバーセキュリティ能力の格差の深刻化としても現れてくるでしょう。

公衆の抵抗 - モラルと倫理の重視

近年はデータ侵害とプライバシー関連のスキャンダルが大きな注目を浴びており、世界中の人々がテクノロジにモラルと倫理を期待していることが実証されました。反倫理的なサプライチェーンや未熟な AI による意思決定が主要なニュースとして報じられ、今後も同様のことがさらに多くなると見込まれています。技術倫理の検討に適した人材の選択さえも、一般の関心と議論を呼ぶ問題になっています。シナリオのストーリーでは、テクノロジを活用して大気汚染や海洋汚染などの世界規模の難題に立ち向かい、大企業はカーボンネガティブの目標を達成し、エネルギーは地域で生産されるという未来が描かれています。今後 10 年間に、全世界の人々がこれらの問題に鈍感になると予測する理由はまったくありません。それどころか、情報セキュリティの専門家が使用するものを含めて、テクノロジの開発においては、プライバシー、環境問題、人権のいずれに関しても「正しい」行動をすることがさらに

重視されるようになると考えられます。今後 10 年間に、倫理の分野での専門知識が、テクノロジ開発における重要な資産になるかもしれません。

法規制のすき間に注意

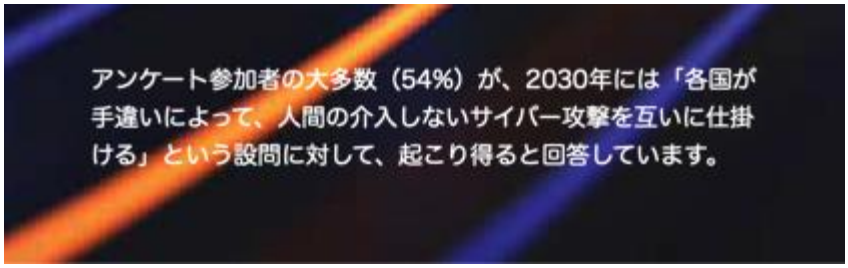
シナリオのストーリーでは、真に AI 対応された暮らしの可能性とリスクについて述べています。この未来では、頻繁に幅広く行われるデータ収集によって、プライバシーに侵入される度合いが高くなります。このため、既存のデータ保護体制がこのような未来に適しているかどうか、また市民をユビキタス監視から保護するために追加の法律制定が必要かどうかを検討する必要があります。さらに、2030 年までに生成されるデータの量に関する懸念もあります。データの処理と保管に関する規制を補完するために、アーカイブ、エージング、整理に関する要件、さらに該当する場合は時間制限を定める必要があります。この要件に対応するために、個人用のアーカイブサービスやレガシーサービスがプライバシー管理市場の分野として登場することが考えられます。

消費者に関係する AI の利用と悪用を抑制する手段、シームレスでありながら一時的な接続が提供されるスマートシティのような環境での調査権の確立など、さまざまな取り組みが必要になりそうです。アンケート参加者の大多数（54%）が、2030 年には「各国が手違いによって、人間の介入しないサイバー攻撃を互いに仕掛ける」（Q.13）という設問に対して、起こり得ると回答しています。この設問自体が、この分野での規制が必要であることを明らかに示しています。参加者の 1 人が述べたように、「この種の危険を防止または軽減するための戦争に関する新たな条約が制定される」と想定することは魅力的ですが、2020 年の多国間サイバースペース統治案に対抗する動きが相次ぎ、テクノロジの導入ペースに規制が追いつかない傾向が持続していることから見れば、自律型致死兵器システム（LAWS）の使用に関して、2030 年までに多国間合意がまとまるという見通しは楽観的かもしれません。

真実、信頼、真正性

2020 年の時点でも、真実、信頼、真正性という一般に認められてきた概念はすでに脅威にさらされています。広く知られた論説によれば、私たちはすでに「ポスト真実」の社会に入っています。シナリオのストーリーに描かれた 2030 年の世界では、市民が事実とフィクションを区別し、正直と不正直を見分けるために役立つ、新しい対策を導入する必要があることは明らかです。ハイパーターゲティングが施されたコンテンツが目の前に提示されると、見ているものに対する反応が強要される可能性があります。すなわち、単に視覚的である、また場合によっては直感的であるという理由だけで、情報の説得力が高まるのです。AI による行動ターゲティング広告は、消費者の意思決定能力を低下させることが考えられます。個人による知識保持のレベルが低下すれば、アクセスしやすい知識への注目度がさらに高ま

ります。デジタル合成の人間が消費およびビジネスの環境において正当に利用されることで、自動化された活動に基づく本物でない行動を特定するツールや、顔の特徴の認証に依存するセキュリティ手段の実効性が低下する可能性があります。市民の批判的思考力を向上させるため、あるいは少なくとも真実の「ポスト信頼」についての認識を促すために前例のない取り組みが必要になりそうです。たとえば、家族のリアルタイムのディープフェイクからライブ電話がかかってきてお金が必要だといわれたら、断ることは難しく、無視することはできないでしょう。同様に、このような説得力のある詐欺ベクトルに対抗するには、技術的に正当性を判断するツールがさらに重要になってくると考えられます。



2030 年とその先の未来

いくつかのテクノロジの発展と影響については、シナリオのストーリーのタイムラインにおいては野心的すぎると判断され、除外されました。最も重要な不確定要素は、量子コンピューティングが 2030 年までに主流となるかどうか、また既存の暗号アルゴリズムを破るのはいつになるかということです。今後 10 年以内に両方とも実現する可能性もありますが、シナリオで近いうちに実現すると述べたのは、未曾有の影響力ときわめて破壊的な潜在能力を持つと考えられるテクノロジについて、詳細に検討することを今回は見合わせるための意図的な手段でした。

Starlink などの低軌道衛星への取り組みにまつわる話題が盛り上がっている現在、シナリオのストーリーに宇宙でのサイバーセキュリティに関する情報をより多く含めたいとも考えましたが、慎重な検討の結果、この誘惑は退けられました。多くの活動の舞台を宇宙に置くと、地球上でのサイバーセキュリティの懸念から気をそらされる危険がありました。圧倒的多数の情報セキュリティの専門家は、地球上でのセキュリティで十分すぎるほど手一杯になっていると考えられます。

ブレインコンピュータインタフェース（BCI）は出現する可能性があるものの、医療でのユースケースを除き、2030 年までに主流のものとしての使用には至らないと見なされました。ヘッドアップディスプレイ（HUD）による印象操作の概念を一歩踏み越え、BCI を標的とすることで、思考プロセスの侵害、すなわち真の「マインドコントロール」が可能になる恐れが出てきますが、今回のプロジェクトで考えられる時代の視野には有り難いことに入りませんでした。身体の完全性に関連するもう 1 つの技術はプログラム可能な細胞組織で、これが 2030 年までに主流になるとは予想されませんでしたが、安全性とセキュリティの問題が生じれば、細胞組織の損傷や疾病を引き起こす可能性があることは考慮せざるを得なくなるでしょう。

シナリオのストーリーで触れたものの詳細には論じなかったのが、人間以外のものが自我を持つという考えです。一般的な想像の中では、ロボットの人権という概念は今から少なくとも 100 年前、カレル・チャペックの時代には確実に存在していました。AI が賢くなればなるほど、この議論がさらに頻繁に聞かれるようになるでしょうが、感覚を持つ AI が登場するまでにはまだ時間が必要で、少なくとも 2030 年よりは先のことでしょう。

付録

シナリオの手法

シナリオのストーリーと、サイバーセキュリティの利害関係者にシナリオが及ぼす影響は、現在の兆候と新興テクノロジの発展を併せて考案されたものです。これは、本書に先行して2013 年に公開された、Project 2020 で使用されたプロセスをほぼ踏襲しています[4]。最初の事例では、2020 年に公開されたサイバー脅威予測の年次報告書を総合したものが、2020 年の脅威の状況のベースライン評価としての役割を果たしました。次に、新興テクノロジに関連する科学論文の抄録、特許、オープンソース資料のレビューが研究チームによって実施されました。この結果、サイバー脅威とサイバーセキュリティの未来に関連した変化の潜在的な推進要因と、主な不確実性が特定されました。

テクノロジの発展と、それに伴うサイバーセキュリティ利害関係者の懸念事項に関するタイムラインの検証は、新型コロナウイルスのパンデミック発生を受けてオンラインに移行しました。招待者のみのオンラインアンケートが、情報セキュリティ、データ保護、国際関係、刑事裁判、その他の公共部門、民間部門、第 3 セクターの専門家に広く配布されました。アンケートは、2030 年までに考えられるテクノロジの発展に関する記述からなる 32 項目の多肢選択問題で構成されました。合計 101 件の記入済みアンケートを受領しました。質問の完全なリストと結果の分析は、本書の巻末に記載されています。

さらに、2020 年 12 月に開催された Pulse CISO360 オンライン会議では、情報セキュリティのリーダーを対象としたライブ投票を実施する機会がありました。ここではアンケート内のセキュリティ運用の未来に関連した質問に焦点が当てられました（QQ.12、13、15、20、25）。投票結果とそれに伴うテキストでの議論の双方がタイムラインの検証に盛り込まれ、シナリオのストーリーの原案をまとめる基礎となりました。

2030 年までに実現する可能性があると認められたテクノロジの発展は、ストーリーに描かれた都市国家、ニュー・サン・ジョバンに変革をもたらした特色として表現されました。これらのストーリーは、2030 年のサイバーセキュリティエコシステムにおける市民、企業、政府の体験の相互接続性、およびより広範な世界的な観点で考えられる展開に対するサイバーセキュリティの関係を説明するものとなっています。相互に接続されたシナリオのストーリー構成により、サイバー脅威と犯罪が企てられる潜在的な機会、サイバーセキュリティの利害関係者に対する影響、およびこの考えられる未来における主な不確実性を明らかにする

[4] Project 2020 の実施方法と結果に関する著者によるレビューは、https://2020.trendmicro.com/review-2020/ に掲載されています。

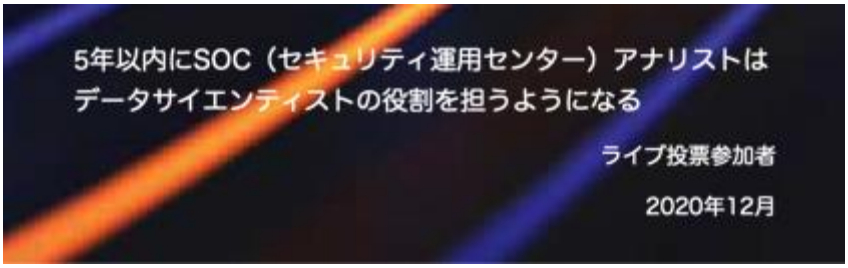
ことができました。これらの点については、このホワイトペーパーのセクション 4、5、6 で論じています。

タイムラインの検証

テストの各記述について、参加者は 3 つの回答から 1 つを選択するよう指示されました。

8. 2030 年にはヘッドアップディスプレイ（HUD）は人間の一部になる

1. 野心的すぎる
2. ほぼそう思う
3. 十分野心的ではない



それぞれの質問について、参考のためにニュース記事へのリンクが提供され、選択について自由に記入できるテキストボックスが用意されました。さらに続く自由記述の質問では、それまでの設問で抜けていたテクノロジの発展、および情報セキュリティの専門家の未来の関心事について記入するよう参加者に促しました。多肢選択問題に対する統計結果は、テクノロジの発展のタイムラインを検証するために役立ち、結果に応じてシナリオのストーリーの草案が修正されました。2030 年の予想としては十分野心的でないと見なされたテスト記述については、特別な注意が払われました。自由回答の内容は個別に検討されました。

Survey Questions

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

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%

図 3：3 2020 年 2 月 12 日に実施された「invitation-only online survey on plausible technological developments」の結果

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%

図 4：CISO 360 のオンライン会議の代表者に対して実施されたライブ「即席」投票の結果、2020 年 12 月

TREND MICRO

〒151-0053
東京都渋谷区代々木 2-1-1　新宿マインズタワー
大代表 TEL：03-5334-3600 FAX：03-5334-4008
http://www.trendmicro.com

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。