Executive Summary

Endorsed by:

ICC UNITED KINGDOM INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

TREND MICRO™

Project 2030 Executive Summary

We tend to be laser focused on the here and now—particularly when we are living through major world events. But we can't let our present focus detract from anticipating how technology will impact our future. Only by carefully calculating future scenarios can the cybersecurity community prepare to protect it.

Trend Micro has taken a futurist view of technology, and its associated cyber threats, that might influence and evolve the world by the year 2030.

This new society may feel like a Sci-Fi film from our viewpoint in 2021. That's how we felt way back in 2012 when we published the **Project 2020 report**. That future felt just out of reach—but it turned out to be a fairly **accurate prediction** of the state of technology and cyber risks today.

Now we repeat this practice to look into the future of society.

The World in 2030

So how will we live and work in 2030? The report looks at the future world from the viewpoint of an individual, an organization, and a government to give a holistic idea of the impact of technological evolution.

Our citizen, Resila, lives in a fully connected world in which the mundane necessities like shopping are fully managed by connected devices and sensors. In fact, nearly everything is connected with sensors to collect data. Nutritional data, gym usage, and sleep patterns are shared with her doctor. Medications are 3D printed, and the connected home has reached maturity. Her son studies digitally, with all information provided through digital lenses, though education is now focused on processing rather than acquiring knowledge. We think of data being king today, but it will only grow in its rule of the world.

Resila works for Konsolidated Rubber and Logistics (KoRLo) Industries, a manufacturing company that has expertly evolved to maintain relevancy. They have synthesized self-healing polymers that are used in extreme conditions, like on the sea floor and in low earth orbit satellites. Sensors in their products report on wear and maintenance needs, predict failures, and provide diagnostics. Industry 4.0 has also reached maturity with fully digitized supply chain monitoring and production lines. All of KoRLo's IT is cloud-based and human employees work only in business strategy, responding to serious anomalies and checking automated work.

This all takes place in the city of New San Joban, a tech-savvy and privacy-centric hub. As with the business and citizen view of 2030, the government is also data-saturated from city-wide sensors. What to do with all the data is a primary concern for the city council, as is ensuring it remains secure. Massive IoT (MIoT) and 5G have connected everything via a SIM, leading to greater technological disparity between sovereign states. The city is cashless, has banned single use plastics, and downtown is petrol-free.

The connectivity and data-driven world has also brought more focus on cybersecurity protections and prosecutions from international committees. However, these regulations and governing bodies are all dependent on the participation and buy-in of individual countries.

Cyber Threats in 2030

By 2030, connectivity will have an impact on every aspect of daily life, on both the physical and psychological level. Malicious threat actors will also evolve to use and abuse technological innovation—as they always do.

Based on the outlined scenarios, criminal activities can be generally categorized as:

- Data manipulation
- Denial of service/disruption
- Extortion
- Influence operations
- Misuse of processing power
- Unauthorized access/intrusion
- Unauthorized data exposure
- Unlawful interception of communications/data transfer

At first glance, these categories seem very similar to what we face today—and the base threats are quite similar. However, automation and AI will change the essence of how these types of attacks function.

Knowledge and understanding are heavily dictated by algorithms and search results, making data manipulation and misinformation highly valuable attack vectors.

Privacy and surveillance issues are a challenge for governments, businesses, and individuals. The benefits of connectivity and data availability can be overshadowed by their potential for abuse.

And the use and abuse of AI to automate attacks and poison datasets can impact all levels of society.

These scenarios and their associated threats will require changes to the business and regulation of cybersecurity. We all, as cybersecurity professionals, must evolve our technology and training to prepare for a future in which everything is connected and at risk.

[SUM00_2030_Report_Executive_Summary_210505US]