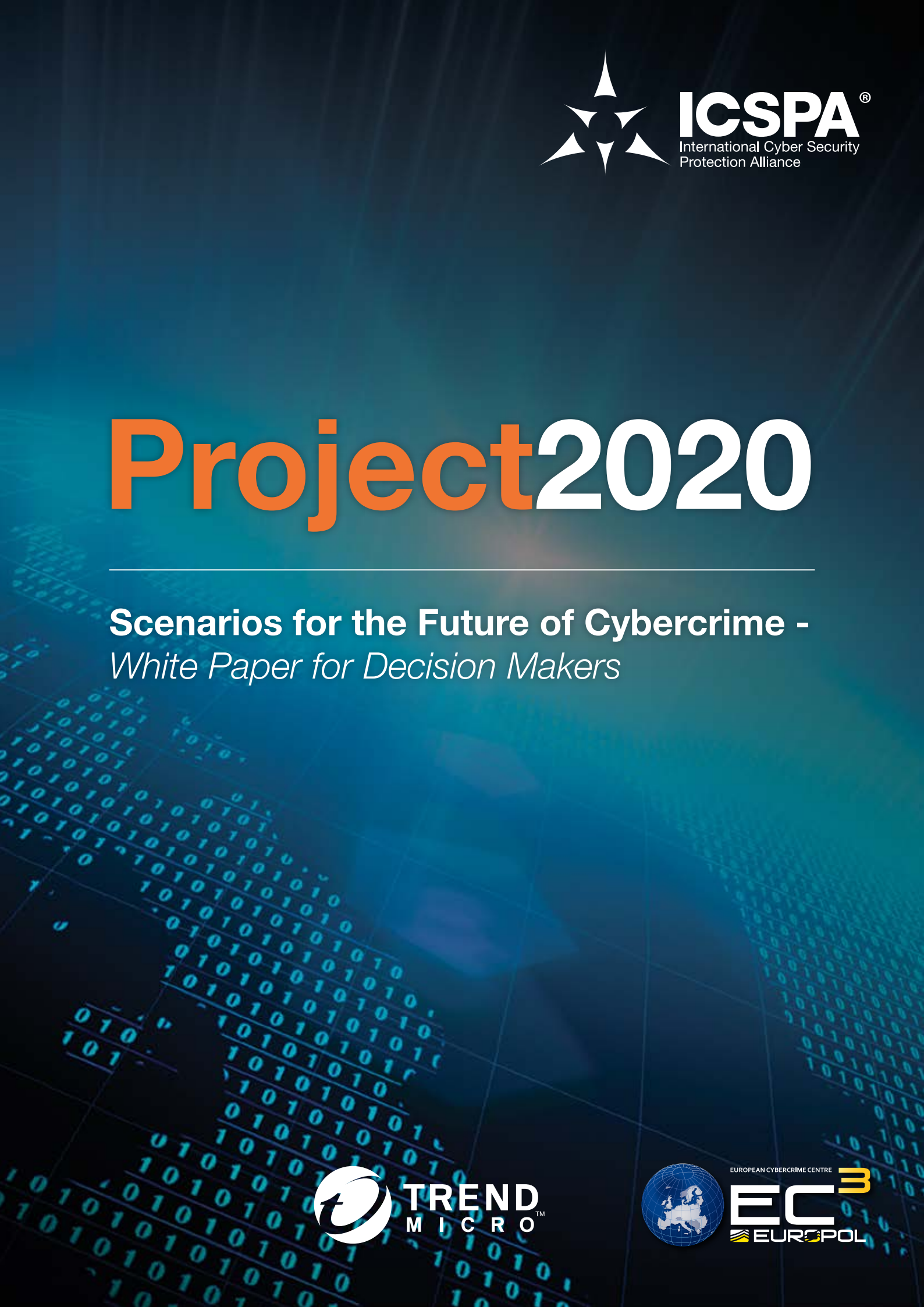
ICSPA®
International Cyber Security
Protection Alliance
Project2020
Scenarios for the Future of Cybercrime -
White Paper for Decision Makers
TREND
MICRO™
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Contents

ICSPA® International Cyber Security Protection Alliance

TREND MICRO™

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

1. About Project 2020

Project 2020 is an initiative of the International Cyber Security Protection Alliance (ICSPA). Its aim is to anticipate the future of cybercrime, enabling governments, businesses and citizens to prepare themselves for the challenges and opportunities of the coming decade. It comprises a range of activities, including common threat reporting, scenario exercises, policy guidance and capacity building.

The scenarios in this document are not predictions of a single future. Rather, they are descriptions of a possible future, which focuses on the impact of cybercrime from the perspectives of an ordinary Internet user, a manufacturer, a communications service provider and a government. The events and developments described are designed to be plausible in some parts of the world, as opposed to inevitable in all. They take their inspiration from analysis of the current threat landscape, the expert opinion of ICSPA members and extensive horizon scanning, particularly of emerging technologies.

The European Cybercrime Centre (EC3) at Europol and the ICSPA would like to express their heartfelt thanks to the Global Review Panel of experts from governments, international organisations, industry and academia who took the time to validate the scenarios. This document is undoubtedly the better for it.

2. Implications for Cybersecurity Stakeholders

The scenarios presented in Section 5 raise a number of questions to be answered by today's stakeholders and decision makers. These include:

- **Who owns the data** in networked systems, and for how long?
- **Who will distinguish between data misuse** and legitimate use, and will we achieve consistency? What data will the authorities be able to access and use for the purposes of preventing and disrupting criminal activity?
- **Who covers** (and recovers) **the losses,** both financial and in terms of data recovery?
- **Who secures the joins** between services, applications and networks? And how can objects that use different technologies operate safely in the same environment?
- Do we want **local or global governance and security** solutions?
- Will we be able to transit to **new governance and business models** without causing global shocks, schisms and significant financial damage?

If these questions remain unanswered, or the responses are uncoordinated, we risk imposing significant barriers to the technological advantages promised by the future described in the scenarios. We are already at decision points for some issues including:

Intellectual Property

The **absolute application of intellectual property rights** has resulted in a "locked down" approach, prompting illegal copying and a market for counterfeit products, and arguably stifling some aspects of creativity. With due consideration for the fact that under the current business model compromise of costly Research and Technology (R&T) potentially entails direct financial losses, loss of competitive advantage and reduced investment, nevertheless the collaborative and (mostly) open nature of Internet connectivity, and the emergence of new "commons" models for licensing, are challenging the way ideas are monetised.

Increasingly, even large corporations are looking to extract value not from their ownership of intellectual property but from the access and usage rights of others. A **major transition from absolute to conditional intellectual property** is possible, but will be highly disruptive to traditional business models in the short- to mid-term, and could well provoke **strikingly diverging policies from governments,** depending on their global standing, economic growth and political systems. The majority of larger enterprises will quite possibly continue to hedge their bets in 2020.

Data Protection and Privacy

Data protection is already a challenge in relation to the Internet. The future reality of large scale Radio Frequency Identification (RFID) deployment, global sensor proliferation, aggregation of data and highly personalised, **augmented services will require the legal frameworks for privacy and security to further adapt.** Existing national differences in viewpoints regarding the privacy rights of citizens could signal the adoption of a variety of approaches to these issues in future. In some countries, misuse of sensor and augmented reality data could become a criminal offence. Likewise, countries may exercise their sovereignty to set their own rules about when such data can be processed and stored by the authorities "for legitimate purposes". **Lack of international approximation will inevitably result in lack of clarity,** and asymmetry in national capabilities for fighting cybercrime.

Identity and Reputation

Reputation will be everything, for governments, businesses and citizens alike. Damage will be instantaneous and increasingly difficult to repair. As indicated in the narratives, the widespread use of multiple identities with varying levels of verification, pseudonymity and anonymity is likely to give rise to new identity management services and tools. An emerging market for outsourced corporate online reputation management is a current signal for this. **Any future lack of consensus on the circumstances under which citizens and the authorities can be legitimately anonymous is likely to result in exploitation of these differences,** including jurisdiction shopping by criminals.

Internet Governance

Lack of unity in Internet governance means lack of unity in cybersecurity. Regardless of the precise number of governance authorities operating in 2020, there will need to be broad consensus on standards, not least to ensure interoperability of emerging Internet mediated technologies, including augmented reality and the Internet of Things.

The rise of hacktivism in recent years serves as a current signal for increasing civil society engagement in issues of Internet governance and data protection. It is anticipated that **citizens will require greater transparency and accountability from their service providers and governments, and autonomy over their data.** Given the pace of expected technological developments such as augmented reality and global sensor proliferation, additional efforts will need to be made to convince Internet users of the trustworthiness of emerging technologies, and their own agency as regards Internet governance.

A truly multi-stakeholder security environment

The scenarios highlight **new tensions and oppositions** in the global cybersecurity environment. Internet connectivity has already fostered the creation of new global networks of citizens, some of which have challenged corporate and government interests. By 2020, civil society networks like these could well be a powerful force in cybersecurity. Equally, effective cybersecurity will require **active risk management by all stakeholders.** But the next seven to eight years could also see **increasing tensions between corporate entities and governments,** particularly in regions where Internet filtering and local intellectual property regimes are deemed to run counter to business interests.

Risk or control? A key tension for the future

The world depicted in the narratives is to a large extent divided into **risk-based and control-based cybersecurity models.** Control models are associated with security through lock-down, heavy reliance on technical prevention, Internet filtering, absolute protection for intellectual property, and sub-optimal interoperability. Risk models, on the other hand, are associated with an open and generative Internet, conditional intellectual property regimes, and exposure to the full range of threats to be found on truly converged networks.

2020 is perhaps most likely to exhibit a combination of these two models. Based on current signals, however, it is possible that their distribution will be rather patchy, with some regions or states exhibiting a large risk appetite and early adoption of new business models, and others doggedly seeking to maintain the status quo or even adopting regressive strategies in order to exert territorial control and serve the perceived interests of national sovereignty.

Countries and corporations opting for more of a risk-based model are going to need more lawyers, more insurance and more cybercrime specialists. All three will be very big business in such an environment. But it may also foster new innovation, investment and employment opportunities in collaborative design and manufacturing, identity and reputation management, risk management and **new approaches to cybersecurity.**

3. Cybercriminal Threats

At the most simplistic level, the cybercriminal threats envisaged in the narratives can be broken down into the following categories:

- Intrusion for monetary or other benefit
- Interception for espionage
- Manipulation of information or networks
- Data destruction
- Misuse of processing power
- Counterfeit items
- Evasion tools and techniques

The vast majority of these threats were already present to some degree in 2012. Targets will range from individuals, small and medium-sized enterprises (SMEs) and corporations to critical infrastructure and defence systems, motivations from sheer amusement (lulz) to profit to commercial and technological advantage and national security. In these respects, at least, **some cybercrimes in 2020 will be adaptations of existing crimes to the technological developments of the next seven to eight years.**

In addition, new challenges will emerge. Evolved threats to critical infrastructure and human implants will increasingly blur the distinction between cyber and physical attack, resulting in offline destruction and physical injury. Moreover, increasing incorporation of augmented and virtual reality technologies into daily life has the potential to result in **cybercrimes which entail psychological harm** to individuals.

In a truly converged 2020, the following cyber-related activities may be more apparent:

- A market for scramblers of mood recognition, remote presence and Near Field Communication technologies
- Highly distributed denial of service attacks using Cloud processing
- A move from device-based to Cloud-based botnets, hijacking distributed processing power
- A mature illicit market for virtual items, both stolen and counterfeit
- Distributed bulletproof and criminal processing
- Physical attacks against data centres and Internet exchanges
- Electronic attacks on critical infrastructure, including power supply, transport and data services
- Micro-criminality, including theft and fraudulent generation of micro payments
- Bio-hacks for multi-factor authentication components
- Cyber-enabled violence against individuals, and malware for humans
- Cyber gang wars

- Advanced criminal intelligence gathering, including exploitation of big and intelligent data
- High impact, targeted identity theft and avatar hijack
- Sophisticated reputation manipulation
- Misuse of augmented reality for attacks and frauds based on social engineering
- Interference with, and criminal misuse of, unmanned vehicles and robotic devices
- Hacks against connected devices with direct physical impact (car-to-car communications, heads-up display and other wearable technology, etc.)

The above list begs the question of exactly **who will be empowered and capable to investigate and combat such threats.** There is already some overlap between investigations conducted by the authorities and those conducted by communications and financial service providers, and Internet security companies. **The capacities of law enforcement and the criminal justice system will need to be significantly enhanced** in order to meet the challenges of cybercrime in 2020. Moreover, the authorities will be required to develop **more creative and flexible responses to criminality,** following the example of existing quasi-judicial sanctions such as asset recovery and crime prevention orders.

The distinction between legitimate and illegal activity may also become increasingly blurred, since practices such as data harvesting and interception, and reputation manipulation will be even more closely associated with profit generation. Current proximity between criminal spamming and legitimate marketing techniques such as behavioural advertising already serves as an indicator for this. The challenge for legislators will be to delineate the circumstances under which these activities may legitimately be conducted, and to ensure that as far as possible these measures are harmonised internationally. Criminalisation will naturally also require sufficient capacity to investigate, disrupt and prosecute.

Finally, **expansion in the use of unmanned vehicles, robotic devices and automation will inevitably raise the issue of whether computers are intelligent agents.** This could be a game changer for criminal law, which historically exists to regulate interactions between human beings.

4. The View from 2012

Systematic review of Internet security industry reporting revealed the following as key features on the 2012 cyber threat landscape:

Cloud/Virtualisation
Consumerisation/Bring Your Own Device (BYOD)
Crime as a Service
Cyber Weapons
Data-Stealing Trojans
Embedded Hardware
Hacktivism
High Profile Data Loss
Industrial Control Systems (SCADA)
Legislation working against security
Malware outside the Operating System
Mobile
New threat actors
New ways to hide
Online Financial Service Attacks
Rogue Certificates
Social Engineering
Social Networking/Media
Spam goes legitimate
Secure Sockets Layer (SSL) & Transport Layer Security (TLS) Attacks
Targeted Attacks
Web Exploits

These not only serve as a general set of current indicators for the evolution of cybercrime, but also enable the identification of a number of horizontal trends to be played out in the future. These include:

- Outsourcing of data storage and processing, and compromise of virtual machines
- Third party access to and protection of data vs. personal control
- Aggregation of data as attractive to criminals
- Apps as dominant delivery mechanisms
- Distributed computing as a criminal tool
- Closer links between digital and physical disruptions
- A redefinition of privacy at the hands of digital natives
- Too much information
- An increase in economic cyber espionage via targeted attacks
- A large pool of unmanaged devices and services in enterprise environments
- Next generation of employees do not feel responsible for security
- Attacks focused on convenience payments and digital currency (Near Field Communication, mobile payments and banking apps, etc.)
- Legislation fails to keep pace with technology and even hinders attempts to improve security
- Distinction between criminal and legitimate methods blurs: criminals monetise legitimate services, while legitimate companies spam

These undercurrents all appear in some form in the scenario narratives in Section 5 of this document. These focus intentionally on the criminal and economic aspects of cybersecurity in 2020, drawing out the dependencies between various technologies and different actors in society, and identifying barriers to progress and effective security.

5. Scenario Narratives for 2020

The world described in the narratives that follow is shaped by two basic assumptions: first, the global availability of mobile wireless Internet, regardless of its divisions; second, persistence of the current dynamic in which technology and the market economy lead where geopolitics and legislation follow.

The rate of mainstream uptake of some technologies depicted in the narratives may seem somewhat ambitious for 2020. This is a conscious choice, which not only allows for a richer and more consistent realisation of emerging technologies, but also reflects the trend observed for the last half century that the pace of technological development outstrips our expectations.

a. Citizen – Kinuko

Key Features:

- Augmented reality and highly personalised content
- Technology assisted living for an ageing population
- Physical threats to the medically vulnerable
- Mature virtual property markets
- Personal data brokerage and identity management
- New forms and patterns of employment

Kinuko is 23 and a second generation digital native. She does most of her shopping online, but when she does go into the city centre she has a highly personalised experience. She doesn't need to window shop, because recommendations for things she's previously purchased or is most likely to be interested in are pushed out to her. This saves her a lot of time and potentially wasted energy – she always knows whether a desired item is in stock before she enters the shop. But she sometimes wonders whether all these tailored recommendations mean she's missing out on trying completely new things.

Of course, it's taken a while for augmented reality to become truly functional. Ten years ago when Kinuko got her first smartphone it was very basic – confined to 2D maps of restaurant reviews and the like. But then the heads-up display (HUD) glasses came along and – even better – the contact lenses. Now Kinuko sees data in 3D right in front of her eyes, and it responds to her gestures so much better than it used to. There's talk online that retina display will be mainstream soon. Kinuko wouldn't go that far, but her little brother and his friends (all 15) don't seem to find it all that strange.

Kinuko's Content Service Provider (CSP) lets her switch off what she doesn't want to see. The premium service is expensive but it's worth it to filter out all the stuff she's not into. Her provider knows that she doesn't particularly like going to bars, so it physically masks them with ads related to her interests – body art, running and collaborative 3D printing projects.

Her display is linked to her social networks, allowing her to spot her friends at a distance, even round corners. This used to be a bit of a pain until she got the premium service, which allows her to render herself – or at least her data – invisible to particular people, or when she doesn't want company. She tried the basic service for a while, but got tired of being disturbed in the street when she had things to do, places to go.

Kinuko never really has to remember much these days. Her content service lets her record and store anything she wants. But she likes to use her physical memory just in case the service goes down, which happens from time to time. There are still plenty of people out there who insist on experiencing the world without augmentation, but they tend to be from older generations who are more comfortable using smartphones. She's heard that the elderly in particular find it difficult to filter out the "white noise" of augmented reality, and can find it too distracting. She's also seen a news feature on a global parent group that is campaigning for an age limit of 8 years and above, claiming an increase in childhood accidents and serious injuries as a result of augmented reality usage.

Data about Kinuko is being collected all the time. She knows this, and accepts that it's part of a trade off which brings greater convenience. Kinuko has grown up with social media, so she doesn't see a problem with publishing data about herself to others. But she's also one of a growing number of people worldwide who want greater autonomy over their own data. That's why Kinuko made sure that her premium service also included a provision for her to receive a weekly report on how her data is used. This has become really important since her provider recently bought a mood recognition software company. Kinuko draws the line at big companies knowing what mood she's in, particularly as she's a sucker for behavioural advertising. She's thought about buying one of the scramblers she's seen advertised, but doesn't like the thought of possibly funding criminals.

Under the terms of her contract Kinuko has also secured permission to sell her own data. Data is big business, it seems, for good and bad guys alike. Data about people's experiences, behaviour and moods are used to develop new commercial products, and to target these at people who might be interested in them. But they're also helping to teach computers how to be more human, and Kinuko's heard that it won't be long before robots are learning about human behaviour from intelligent data like hers.

Selling her data is something that Kinuko's only very recently been able to do. With all the services out there that generate and store data on people there's been something of an outcry, with citizens reclaiming ownership of their data. Faced with global popular pressure, service providers have offered certain premium customers the ability to resell their data. As a result specialist data brokers are springing up all over the world. But it can be difficult to tell the legitimate companies from the bogus ones, especially in some regions, and now there are calls for greater regulation. Kinuko uses a recognised identity and reputation management service as a data broker, which takes commission every time she transfers 1 Gigabyte (GB). In return she gets micro-credits, which can be used at most retailers.

This company manages multiple identities for Kinuko, with different levels of anonymity. There is her official identity, which she uses to vote, pay taxes and fines (mostly for traffic offences in Kinuko's case), her three social identities (for family and friends, gaming, and everyone else) and her two business identities (manufacturing and music). After she had her main bank account hacked five years ago Kinuko decided to have a different payment system for each of her identities. It spreads the risk, but keeping track of everything can be tricky. Luckily, her identity management service does that for her too. It also monitors her "presence" and reputation, alerts her when she appears in any content and flags up behaviours from sensor data that she may not want to share with others.

For Kinuko's generation, visiting a branch of a bank is a distant memory, as are weekly visits to a supermarket. For years now Kinuko's finances have been managed entirely online, her payments entirely mobile. It can sometimes be a bit of a chore verifying all her transactions, but the iris and voice recognition apps speed things up a bit.

Kinuko doesn't have a full time job, but gets enough to live on from a number of part-time interests. She runs a manufacturing business with a group of colleagues she met on a project-based recruitment site, making parts for gadgets and children's toys using 3D printing technology. The team is located all over the world, and they design, project-manage and manage their finances in the Cloud. To generate extra income, the team sublets its processing power when not in use.

Kinuko also belongs to a barter network where she trades her skills and knowledge. She's an accomplished guitarist, and the online lessons she gives generate credits, which she can trade in for the help she needs with her technical designs. She's also collecting micro-credits for her online performances, but sometimes she donates to good causes herself, helping to kick-start the production of a movie or a book which sounds interesting. She spends a lot of money on in-game items – too much, her Mum says. But she's only got stung with counterfeits once or twice and she's not had any items stolen so far this year.

Kinuko is single at the moment, but she's just signed up to a new dating service, which uses her personal and sensor data to match her with someone who is behaviourally similar. She's got an online date with a guy in Mexico this evening. She doesn't speak Spanish, but instant translation is now so good that that shouldn't be a problem.

Much of the data associated with Kinuko is generated by sensors, which report remotely to other machines without her noticing. Her car transmits data on its state of repair to her garage, her essential food and household items are automatically reordered when they are used up, and her home reports on its energy and data usage. Even some of her clothing items are fitted with sensors – when she goes to the gym they collect data on her heart rate and workout performance, so her online trainer can monitor her fitness and adapt her tailored program accordingly.

Kinuko doesn't mind wearing sensors, but she draws the line at having an implant. That's the way things seem to be going in some countries, with RFID tagging at birth. The governments concerned say it's for public safety and convenience, but plenty aren't convinced. And yet, wireless implants seem to be starting to catch on amongst gaming communities elsewhere. The only problem is that some gamers are already being infected with malware.

Since smart grids came online a few years ago Kinuko has heard that in some parts of the world people are able to steal electricity by hacking into the system. That's bad enough in itself, as there's always a poor consumer who's losing out, but it's even worse in areas where the power and Internet connection are delivered down the same tube. In these places, one hack can mean stolen electricity and personal data at the same time.

But when Kinuko thinks of her great-grandfather she's actually quite happy that so many things are now networked. Felix is 94, lives on his own, and is one of the many people who now benefit from technology assisted living. Medical implants regulate Felix's heartbeat and blood sugar levels, reporting wirelessly to his medical service provider. His home is specially adapted to keep him safe and healthy – turning off his gas stove after an hour unless he overrides it, only filling his bath for a specified amount of time, adjusting the climate to his body temperature and prompting him to update his social media status every two hours so that his family and friends know he's OK.

Kinuko does worry about what would happen if someone were to interfere with Felix's home management system. Every six months or so there's a data outage of some kind – it seems the data centres get overloaded sometimes, that the different types of sensor aren't always compatible with each other. There have even been terrorist attacks on data hubs that have resulted in elderly people falling seriously ill. But Kinuko also suspects that Felix doesn't really understand how to keep his home network secure – he's always falling for scams, and he doesn't always know how to tell a legitimate home management app from a malicious one designed to steal his data. So she's adding him to her account with her risk management provider.

b. Business *- Xinesys Enterprises (SME) and Lakoocha (CSP)*

Key Features:

- Enterprise virtualisation reaches maturity
- Supply and distribution chain automation
- New approaches to intellectual property, and Research and Technology (R&T)
- Greater storage of data = greater liability
- Communications as critical infrastructure
- Security scores as indicators of trustworthiness
- A dedicated Internet for secure payments

Xinesys Enterprises is a small to medium-sized enterprise with just under 200 full time employees worldwide. It punches above its commercial weight thanks to recent supply chain and distribution innovations. Amongst its portfolio Xinesys produces mid-tech devices that assist in and benefit from smart home technology. Their best selling product is the R0Bud, a robotics-based gadget which many consumers buy as a toy, but which has come to be something of a home help for those with limited mobility. Lakoocha, meanwhile, is a world leader in communications (and now also content) provision.

Although officially Xinesys is classed as a manufacturer, their activity is more accurately described as assemblage. Parts for the R0Bud are produced in various locations by smaller concerns: its wheels are made by Kinuko and her team. The Xinesys business model is heavily reliant on automation: goods are checked in and out of its warehouses automatically, and items in both the supply and distribution chains are transported without direct human intervention. Components in transit contain executable code which enables them to make intelligent decisions about their transport and receive routing instructions from their dispatcher. This greatly improves efficiency, but restricts the company's choice of suppliers to those who have already embraced this technology.

This supply and distribution method also comes with its own risks. Xinesys accepts that a certain amount of its stock will go missing in transit. While some of this can be attributed to accidental misrouting, it is clear that in some cases a new kind of theft is being committed, with criminals intercepting and rerouting stock for retail on the black market. Highly sophisticated underground Research & Technology (R&T) has also resulted in the production of counterfeit tags and sensors with sub-optimal performance, which ultimately disrupt effective transit.

New business models continue to challenge traditional notions of intellectual property. Some large corporations who continue to insist upon absolute intellectual property rights are finding themselves left behind by those who make their R&T available to the commons under certain conditions, thereby encouraging open source and user generated innovation. Various different models and new regimes are springing up around the world, and while Xinesys naturally wants to protect its intellectual property, it has already seen positive results from making some of its own R&T available for further open source development, e.g. by paying distributed design collectives to contribute to the evolution of existing products, and the development of new profitable uses for existing technology.

Both Xinesys and Lakoocha have grown used to nuisance attacks, which are an occupational hazard of being a public facing company. Corporate websites and feeds remain at risk of getting "owned", and this practice is now so common that it's almost become part of the fabric, Internet graffiti. But attacks for the lulz are increasingly sophisticated – in recent months Lakoocha in particular has been the victim of fake press releases designed to ridicule the CEO and intrusions with no apparent motive other than to undermine confidence by manipulating data. In Xinesys' line of work, there have been instances of anti-sec activists posing as legitimate suppliers in order to undermine the effectiveness of products and automated supply chain distribution.

Even the smallest concerns now insure against data loss and associated reputational damage, and cyber risk insurance is a legal requirement in many countries. The imposition of security scores for corporate entities is a mixed blessing. There is no doubt that it encourages greater social responsibility and public confidence, but it has also meant that the CEOs of both Xinesys and Lakoocha have had to justify much higher expenditure on reputation and risk management. For smaller enterprises like Xinesys, there are specialist risk management companies of security consultants to which this task can be outsourced. Large multi-nationals like Lakoocha, on the other hand, have for the most part chosen to bolster their existing information security departments.

The Universal Security Score system is in fact quite useful when it comes to vetting prospective suppliers and distributors. The advent of "business in a box" cloud services has facilitated the establishment of bogus companies with the intent of stealing product, personal data and R&T. Where once professional looking web pages gave an air of legitimacy to criminal enterprises, now scam merchants can purchase an entirely legitimate infrastructure and set of business processes at very low cost.

The stakes are high. For all that large corporations have been able to secure their stand-alone databases, convergence of data from different sources over a global wireless network also engenders converged threats. And in a world where reputation has become everything, compromise – particularly of customer data – has an immediate impact on share prices and consumer confidence.

For this reason, established banking and payment providers are leading the way in the creation of a dedicated Internet for secure transfers. This has in turn created something of a headache for businesses like Xinesys, whose operations necessarily straddle the "secure" and public Internets, and has prompted the emergence of bridging services. Inevitably, bogus bridging services have appeared which harvest data for retail in the digital underground.

There is now such a plethora of payment systems, some running on the "secure" Internet, some not, and so far no single architectural solution has held sway. The situation is equally challenging for Lakoocha, which must deliver to consumers mixed streams of data from different clouds without compromising security.

Communications and content service provision is now firmly classified as critical infrastructure, especially in those countries where power and data are delivered together. This has drawn large service providers further into matters of international diplomacy. Companies like Lakoocha with operations in a number of different countries find themselves variously subject to state regulation or self-regulation, and having to deliver very different services accordingly. Such is the control of the Internet in some countries that it has become virtually impossible for some (less preferred) multi-nationals to operate.

Xinesys has naturally moved its processing to a Cloud provider. Inevitably there was some initial concern from the Board and shareholders about this degree of outsourcing, but a stringent service level agreement – stipulating the exact circumstances under which the provider may use the company's data – and round the clock scrutiny from the contracted risk and security management service has gone some way to allaying these fears.

To date, Xinesys is not aware of having experienced any major breaches, which is just as well, as it has seen the impact service disruption and data theft has had on some of its competitors. Outages, be they by design (infrastructure maintenance), malicious (Denial of Service) or by accident, are an unfortunate reality of distributed computing, but the provision of geographically distributed back-up locations in Xinesys' service level agreement means that these are largely temporary, with most disruptions lasting no more than a couple of minutes. Nevertheless, social engineering of employees continues to be a successful attack vector, and the wholesale enterprise adoption of social media has increased the attack surface. This is a world in which botnets have moved to the Cloud, and Xinesys personnel access their virtual work machines from any number of devices.

The issue of liability is increasingly complex. Companies like Xinesys and Lakoocha already have arrangements in place for the processing and storage of personal data. But the global proliferation of sensor data and the delivery of personally augmented content means that much larger amounts of data are vulnerable to compromise, and this data is potentially much more revealing about individuals.

Because in many places the Internet has become so personalised, consumers now find it much easier to filter out unsolicited advertising. Xinesys therefore relies on pushing content to CSPs in order to generate business, in addition to traditional web-based advertising. Advertisements and marketing material is then relayed to potential customers via augmented reality and context-based services.

All this data has an intrinsic value. There are companies who retail big and intelligent data, which enable service providers both big and small to identify and target potential customers based on their behaviour. But questions have arisen concerning the methods some companies use to obtain this data, and in a number of cases criminal groups have been found to have supplied legitimate service providers.

Individuals who discover – often through their identity management services – that their personal data has been compromised or even misused, increasingly sue CSPs and other large corporations. Meanwhile, communications providers like Lakoocha are finding themselves accused of negligence regarding attacks on critical infrastructure and responsibility for physical injury to individuals when service interruptions impact on the functioning of wireless enabled medical devices. Transparency is the watchword, as many consumers become obsessed with the small print of their contracts and privacy policies, and seek high levels of accountability from their service providers.

In terms of business processes, multi-nationals are just beginning to experiment with remote presence technologies. Advances in virtual reality facilitated by 3D tracking, cognitive neuroscience and haptic interfaces have enabled the development of technology that maps speech and behaviourisms onto virtual or robotic representatives, potentially succeeding in remote business interactions where video conferencing and virtual worlds have failed. After the initial outlay, implementation is of course much more cost effective than flying executives around the world to face-to-face meetings, and there are precedents for its performance in the military, nuclear power generation and gaming. But it remains to be seen whether corporations heavily reliant on trust and personal relationships will take to it, and there have already been incidents of criminal interception, manipulation, and eavesdropping for profit.

c. Government - South Sylvania

Key Features:

- New tech powers, and R&T "leapfrogging"
- Internet diplomacy and international diplomacy one and the same
- Countries with lower levels of cybersecurity become "no go" areas, and havens for cybercriminals
- Increasing tensions between governments and multi-national corporations
- Attacks on critical information infrastructure result in physical destruction and violence (integrated transport networks and energy supply)
- Citizens demand greater government transparency - increasing focus on reputation management in government administrations

The Republic of South Sylvania is a middle income, emerging market with an abundant supply of natural resources, including rare earths. Before the crash of 2007-8 it enjoyed consistent economic growth due to a global commodities boom. Afterwards GDP recovered relatively quickly, and the country now appears to be enjoying a period of steady and sustained growth

This has prompted an improvement in living standards. Twenty years ago 50 per cent of the population lived below the poverty line: that figure has now halved. Foreign direct investment in the country has undoubtedly boosted growth, but has also altered the domestic balance of power. The rare earths so necessary for the last decade's technological advances such as electric cars are rapidly depleting. This has engendered a scramble by multi-national corporations, inflating the price of the minerals, but also making South Sylvania somewhat beholden to their interests.

Fortunately, the previous Finance and Enterprise Minister ensured that the country began to diversify its portfolio of goods and services some years ago. He insisted that the government invest in technological innovation and education, and now South Sylvania is both a world leader in mobile payment systems, and a regional hub for innovation. It has also benefited from its location at the crossroads of several large cable networks, and the eventual roll out of global high-speed wireless networks.

Like a number of previously under-connected countries, South Sylvania has leapfrogged many other more developed nations in terms of Research and Technology (R&T). The world's leading online design university is hosted in its capital, and the South Sylvania Technological Institute is at the forefront of nano-tissue development, which is expected to be in mainstream medical use within the next couple of years.

But these remain uncertain times, particularly due to large disparities between different parts of the world in terms of economic growth, innovation and access to information. South Sylvania has a comparatively liberal government, which does not engage in Internet filtering. As a result, citizen experience is personalised and augmented by content providers in industry.

Many of the citizen-facing government functions traditionally performed by personnel have now been entirely automated. These include voting (now entirely online), taxation, and some aspects of policing, in particular surveillance. Sensors and Radio Frequency Identification (RFID) track citizen movements, while advanced behavioural profiling helps intelligence operatives to identify individuals at risk of engaging in criminal or terrorist activity. Greater automation and artificial agency is exercising legal experts, as the question of whether computers and robots can be criminal agents becomes increasingly pertinent.

The demand for greater transparency in the government-citizen relationship, and the continued rise of global popular movements online has made the government's reputation highly vulnerable to criticism, however unfounded. Where hacktivism once contented itself with defacing or denying service on a website (DDoS), a new generation are engaged in tech-enabled destruction which appears to be motivated by anarchist as well as anti-corporate sympathies. Automation of some law enforcement functions has also inevitably attracted attempts by criminals to gather intelligence, manipulate data and obstruct access.

Global networks of opponents to centralised sensor and RFID tracking have conducted physical attacks on data centres identified – often erroneously – as storing this information. One such attack was committed in South Sylvania just last year, resulting in damage to the tune of millions of USD, temporary loss of functionality in various parts of the world, and reduced international confidence in South Sylvania as a secure location.

Press statements and riot police are no longer sufficient to quell unrest and public disorder. While some governments have chosen to lock down their domestic Internets, South Sylvania has instead opted to substantially increase its civil service public relations contingent. A veritable army of employees works full time to optimise the government's online presence, and to respond to the concerns of citizens and global groups.

The government is currently under substantial popular pressure to restrict corporate data harvesting, and to impose standards for the retention and safe storage of personal data after a number of high profile hacks. Meanwhile, a number of politicians who once espoused hacktivist ethics are now members of national governments as Ministers for Freedom of Information. But for those members of society who are content to be convenience-led consumers, power and data outage is the biggest concern: such is the dependence of citizens on network-mediated content that data blackouts threaten to erupt in instances of public disorder.

The emergence of different regional Internets frustrates international diplomacy. It is no longer merely the case that hostile states block access to services hosted in another country which they deem to be undesirable. Dissident anonymised access and distributed processing is also being targeted, with denial of service (DoS) attacks by states on service providers, wherever they may be hosted. Some states in which these services are registered have described these attacks as acts of war, highlighting the fact that ubiquitous and distributed computing is now part of the global critical infrastructure.

International diplomacy and Internet diplomacy are now one and the same. Allegations of state on state attacks are increasingly brought before the UN Security Council and General Assembly. An International Treaty for Cyberspace was concluded three years ago, detailing the rules of state on state engagement and a basic code of conduct. An International Cybercriminal Court has also been established, which to date has heard only a handful of cases.

The Court has extra territorial jurisdiction but can only exercise this if mandated by a unanimous decision of the UN Security Council. States have been reluctant to waive their sovereignty over eligible cases and the Security Council has not been able to agree between its members. Moreover, there have been difficulties recruiting and appointing prosecutors, judges and defence counsel who are suitably qualified and experienced in the field of cybercrime. Timely attribution is also proving increasingly difficult in a world of distributed computing, where the vast majority of attacks originate from the Cloud. In addition, the Court was unprepared for the increase in cyber espionage between corporations and governments.

In practical terms, responsibility for Internet governance lies with the Internet Authority, a multi-stakeholder community with representatives from government, industry and civil society groups. This group has evolved organically over the last thirty years, and is the most effective forum for achieving consensus over norms and standards. But it remains a coalition of the willing, and notable absences have so far prevented the setting of truly global standards and interoperability. There is hope, however, that in the near future the few remaining states and service providers will come to actively participate, thereby enabling the Internet of Things to realise its full global potential.

South Sylvania's critical infrastructure is entirely in the hands of the private sector, but there remains an expectation from its citizens that the government will retain oversight of aspects that affect their personal safety. The government has a clear interest in ensuring the efficiency and security of transport networks, power and data supply, and works with service providers to optimise security provisions and minimise vulnerabilities, mostly through the issue of minimum standards and fostering good practice in self-regulation. But the government is well aware that there is no such thing as absolute security. Both the movement of industrial control systems to the Cloud and consumerisation of their operation through apps and other platforms have brought new risks of interference and manipulation.

One highly publicised incident in the state of Catistan has served to highlight the extent to which critical infrastructure is vulnerable to external interference in some parts of the world. A few months ago a gas pipeline running through a densely populated area of the country ruptured, killing and injuring a number of local residents. The latest reports have attributed this to corporate espionage, more specifically a deliberate attempt by a competitor to undermine confidence in the supplier by remotely manipulating the pipeline's pressure sensors. This has had a direct effect on Catistan's reputation, with perceptions of poor digital hygiene already affecting levels of foreign investment.

Stand alone systems in private networks have tended to be less vulnerable than, for instance, the transport network, which combines public transport RFID fare data with car sensor reports and traffic control systems. An integrated system was rolled out in South Sylvania's capital city four years ago. Within two years, an anarchist attack on the control centre had resulted in traffic chaos, and a number of deaths as a result of road accidents and underground railway collisions. Jamming of the emergency services network exacerbated the crisis, as did an outage of RFID passenger data, which meant that first responders had no idea how many citizens were affected until a number of hours after the first incident. In wealthier economies, unmanned aerial vehicles (UAVs) and robotic surveillance devices assist urban transport networks. While South Sylvania aspires to similar advances, it is waiting to see how securely these can be implemented, and whether they meet with sustained public acceptance.

Converged networks are only as strong as their weakest link, and governments around the world have realised that technical security measures for individual platforms and devices are no longer sufficient to meet threats that arise from the convergence of data from different types of service. Along with a number of other countries, South Sylvania has put its support behind the Universal Security Score initiative, which assesses the trustworthiness of businesses and individual citizens, based on a combination of factors including the number of scams to which they have fallen victim, the extent to which they have unwittingly propagated malware or facilitated cybercrime and how securely they store their personal or customer data.

Citizens and businesses are increasingly rated and insured according to this score: poor digital hygiene is linked to high premiums and, in some countries, denial of access to secure services. There has been talk of governments also being accountable in this way in the future, but there are concerns that this will merely result in signatory states yielding valuable intelligence about their network and information security to hostile states with no intention of participating.

In terms of national security and law enforcement, South Sylvania's considerable investment in technological innovation and education has resulted in a large employment base. Traditional forms of crime have become increasingly technology enabled: there are already gangs of domestic burglars who select their targets using compromised sensor data retailed in underground forums, and ATM skimmers who know which machines have the most cash at any one time. Meanwhile cybercrime itself continues to be consumerised: the digital underground economy not only provides bullet proof cloud processing, but also specialist criminal apps for intelligence gathering, data harvesting operations, intrusion and manipulation, denial of service, and command and control.

Equally, expansion in forms of intrusion, data manipulation and destruction demands that larger numbers of law enforcement and security operatives possess the requisite technical skill to disrupt such activity. Countries that failed to invest in this capacity five years ago are now rapidly becoming "no go" areas for secure transactions and safe havens for the cybercriminal fraternity.

Virtual currencies have been popular for a decade or so. The decision of some countries to develop government issued variants has prompted moves to establish a global virtual currency. This is enthusiastically supported by smaller countries with lesser-known hard currencies. Indeed, in light of crises in some of the "big" currencies in the last ten years, the Ochip, as it is currently known, is also seen by a few emerging economies as a viable alternative to which to tie national currencies. Confidence in the initiative is inevitably closely linked to its security: a large intrusion, which made away with millions of Ochips eighteen months ago, has resulted in delays to the programme. It remains to be seen whether it has also caused lasting harm to the Ochip's reputation.

6. Beyond 2020

For all the developing technology that may be in mainstream usage by 2020, there will equally be technology emerging in 2020 that will not see widespread adoption for some years. Remote presence and virtual reality technologies will perhaps only just be coming on to the mainstream market, meaning that their potential for legitimate use – and criminal misuse – will not be fully realised in the time frame of the scenario narratives. It is reasonable to speculate, however, that the level of interaction of truly immersive technologies with human cognitive processes will bring new harms (especially psychological) as well as benefits.

In 2012, medical implants such as defibrillators, pacemakers and insulin pumps already report wirelessly. By 2020, we will be a number of steps closer to Ray Kurzweil's "singularity" of man and machine. While the vast majority of today's Internet users would baulk at the idea of receiving a brain or retina implant, mainstream adoption of augmented reality, virtual reality and sensor technology may prime 2020's younger generations for uptake, and desensitise them to some of the possible attached risks.

Finally, in 2020 quantum computing is just on the horizon. And quantum computing is probably going to change everything…

Appendix – Scenario Method

The above scenarios and their implications for cybersecurity stakeholders have been elaborated on the basis of a combination of current signals and emerging technological developments, according to the following process.

In the first instance, a synthesis of current reporting from a range of Internet security companies served as a baseline assessment of the threat landscape in 2012. This was provided by ICSPA member organisation Trend Micro.

Next, a review of scientific abstracts and open source material relating to emerging technologies was conducted by a team of subject matter experts, threat analysts and legal specialists at Europol. This resulted in the identification of potential drivers for change and key uncertainties related to the future of cybercrime. It was complemented by findings from two multi-stakeholder workshops held under the auspices of the ICSPA, and further research on both the future of the Internet and anticipated social, economic and geopolitical developments.

Elements were then mapped as a network of interdependencies, thereby enabling the identification of criminal opportunities, vulnerabilities and unanswered questions concerning such aspects as legislation, governance and interoperability. These became the building blocks of the scenario narratives, which have been elaborated intentionally to illustrate the interconnectedness of citizen, corporate and government experiences in the cybersecurity ecosystem of 2020, and the relationship of cybersecurity to potential developments in the wider global context.

A draft of the scenarios was circulated to a Global Review Panel of experts in governments, international organisations, industry and academia. This panel reviewed the scenarios and provided additional guidance on both their implications for cybersecurity stakeholders and the specific cybercriminal threats presented.

ICSPA®
International Cyber Security Protection Alliance

If you are interested in finding out more about the work of the **ICSPA,** please contact:

Linda Bentley
Business Development Coordinator
+441494798160
linda.bentley@icspa.org

or visit our website:
www.icspa.org

International Cyber Security Protection Alliance
Copsham House
53 Broad Street
CHESHAM
Buckinghamshire
United Kingdom
HP5 3EA

TREND MICRO™

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL