TREND MICRO™

The Benefit of Foresight

Project *2020* in Review

Dr. Victoria Baines
Visiting Research Fellow, Oxford University

Rik Ferguson
Vice President Security Research, Trend Micro

Inside This Report

Abstract

In 2012, a project led by Europol's European Cybercrime Centre (EC3) and Trend Micro sought to anticipate the future of cybercrime in 2020. Building scenario narratives for governments, businesses, and citizens—and dramatizing these as a series of short movies—the project envisaged a near to mid-term future in which technological developments created both new possibilities and new threats.[1] As we enter the 2020s, we have the opportunity to review the project against a number of success factors. What did we get "right" in terms of technological developments and implications for cybersecurity? Did we use a robust and appropriate method for the task? And if we were to do it again, would we do it the same way? This paper explores these questions and more.

[1] https://icspa.org/project-2020-scenarios-for-the-future-of-cybercrime/; http://2020.trendmicro.com

1. Context

1.1 About Project 2020

Project 2020 emerged from discussions among members of the International Cyber Security Protection Alliance (ICSPA), a not-for-profit organization whose members include national and international law enforcement agencies and representatives from the cybersecurity industry.[2] Europol undertook to convene an in-house team to build scenarios for the possible future of cybercrime, inspired by an earlier project on the future of organized crime[3].

In the first instance, Trend Micro provided a synthesis of existing cyber threats in 2012, to serve as a starting point for consideration of their evolution. This is summarized as *The View from 2012* in the *Project 2020* white paper.[4] Europol's project team then reviewed open source material and scientific abstracts on emerging technologies, clustering them into themes that would allow us to consider, for example; the impact of the internet of things (IoT) on logistics, integrated transport systems, and healthcare. It was from these clusters and intersections that the features of the world described in the scenario narratives emerged.

A conscious decision was made to portray the impact of technology and its attendant risks on a number of different actors. Dedicated narratives were drafted for individual citizens (a digital native and her great-grandfather), businesses (a small andmedium-sized enterprise, and a large communications provider), and a fictional government (the Republic of South Sylvania). In the process of drafting, a number of questions and key considerations presented themselves repeatedly. These became their own section of the white paper, *Implications for Cybersecurity Stakeholders*. Finally, recognizing that technological development is continuous and that 2020 would by no means be an endpoint in any real sense, the white paper included a very brief discussion of technologies deemed out of scope for the project's timeline, such as mainstream adoption of virtual reality (VR), and quantum computing.

---

2 https://icspa.org

3 https://www.europol.europa.eu/publications-documents/organised-crime-energy-supply-scenarios-to-2020; https://www.shell.com/energy-and-innovation/the-energy-future/scenarios/meet-the-shell-scenarios-team.html

4 https://icspa.org/project-2020-scenarios-for-the-future-of-cybercrime/

Expert opinion was canvassed at two points in the scenario process. Before drafting the scenario narratives, we tested our clustered signals, themes, and timelines for emerging technology adoption with cybersecurity practitioners at a workshop hosted by the ICSPA. At a later stage, the draft narratives were reviewed by a smaller panel of government and industry practitioners from the ICSPA membership.

1.2 A Very Brief History of Futures Thinking

"Futures thinking", or the application of foresight, is simply the practice of looking ahead and giving due consideration to inevitable change. While some academic researchers locate the origins of futures thinking in ritual attempts to foresee coming events such as divination and astrology, the modern discipline grew in the mid-20th century out of the need, particularly in public policy and business environments, to anticipate changes in the wider world that could impact on an organization's operations, efficiency, profits, and the like. It is no coincidence that futures thinking as a planning tool was first popularized in military departments (RAND) and large corporations (Shell International).

In a parallel evolution, fiction writers have increasingly come to consider the future or alternative worlds. From the fantasy writers of Ancient Greece and Rome, through the development of science fiction at the hands of Jules Verne and H. G. Wells in the 19th and early 20th centuries, to the plethora of future-oriented novels, movies, and TV shows of the late 20th and early 21st centuries, we have, to some degree, all become futures thinkers. The technology press is full of predictions that science fiction writers "got right", including the use of debit cards (Edward Bellamy) and video chat (E. M. Forster). More often than not, the architects of our future are science fiction fans. When we hear that electronic tablets are rumored to have been inspired by props in Stanley Kubrick's *2001: A Space Odyssey*, when a national telecoms provider bears the same name as the rogue artificial intelligence in *Terminator*, and when a meal replacement drink appears to pay homage to a dystopian cannibalistic future, our collective imagination is directly shaping the future more than ever before.

The futurists of the 1960s took the year 2000 as their horizon. In 1967, Herman Kahn's and Anthony J. Wiener's best-selling book of that name presented "a framework for speculation on the next thirty-three years". One year later, Arthur C. Clarke and Stanley Kubrick concurrently produced the novel and film of *2001: A Space Odyssey*. This not only extended foresight efforts to date by looking beyond the landmark year 2000, but also put computer technology (and specifically artificial intelligence) at the heart of that future. As popular as Kahn's thinking was at the time, Kubrick's undoubtedly reached a larger global audience.[5]

[5] It is undoubtedly no coincidence that Kubrick's character of Doctor Strangelove is reputed to be based to some degree on Kahn. For more on this, see https://www.newyorker.com/magazine/2005/06/27/fat-man.

In recent months, the technology and mainstream media are awash with the predictions from another historical view of the future. We have now passed "peak Blade Runner", insofar as the movie was set in November 2019. Recent press coverage has sought to highlight what Philip K. Dick and the movie's writers "got right" or "got wrong".[6] Reconsideration of the movie's features and preoccupations has prompted further reflection and debate on our technological future—artificial intelligence, what it means to be human—and on humans' treatment of the Earth. Review of futures past doesn't just provide entertainment, it allows us to take stock of our present and our progress to the next horizon.

The bulk of what futures thinkers do now is a combination of forecasting based on (sometimes linear) projections, and a more creative process of imagining what alternative future worlds could look like, based on the interaction of certain critical uncertainties. Arguably, they animate the often-dry approach of planners and economists with the flair and liberation of science fiction. Futures exercises are therefore a curious synthesis of art and science.

1.3 Techno-Futures

There is a long history of foresight focused on technology. At the turn of the 20th century, H. G. Wells' *Anticipations of the Reaction of Mechanical and Scientific Progress Upon Human Life and Thought* opened with a forecast on locomotion and the economic, social, environmental, and military impact of the "mechanical revolution". As Daniel Bell notes, "Wells was one of the first writers to see the importance of technology and to derive social consequences from specific innovations. (In contemporary jargon, he relied on this as his independent variable.)".[7] In relying on technology as our independent variable, *Project 2020*'s vision of the future appealed to an established heritage.

Prominent futures thinkers have observed how technological change can accelerate other changes. In his book, *Future Shock*, Alvin Toffler identified technology as "that great, growling engine of change … This is not to say that technology is the only source of change in society. Social upheavals can be touched off by a change in the chemical composition of the atmosphere, by alterations in climate, by changes in fertility, and many other factors. Yet technology is indisputably a major force behind the accelerative thrust".[8] Technology is also generative. As noted by Olaf Helmer, "the occurrence of one development may raise the probability of occurrence of another either because it facilitates the other technologically or because it makes the other

[6] https://www.vice.com/en_us/article/qvgyap/the-future-is-now-what-blade-runner-got-right-and-wrong-about-2019; https://www.bbc.co.uk/news/technology-50247479; https://www.businessinsider.com/blade-runner-movie-predictions-about-2019-technology-it-got-wrong-2019-11?r=US&IR=T

[7] Bell in Kahn & Wiener (1967) xxiii

[8] Toffler (1970) 32

socially more desirable".[9] This has the effect both of making it more challenging to forecast technology's future impact accurately, and of rendering technological foresight essential:

> **"The accelerating rate of change in electronics technology makes it almost impossible to say much that is interesting about the electronics technology of the year 2000. Almost all of the possible developments that once can explicitly formulate seem likely to be realized much sooner."**[10]

> **"Interest in the future has grown rapidly in recent years, because social and technological change is occurring so rapidly that it is apparent to everyone that in as little as 10 or 20 years we will be living in a world vastly different from the world of today."**[11]

Projecting technological developments by a certain date enables the creative process of envisaging mainstream adoption of these technologies and how these might be misused by criminals. The futures thinkers of the 1960s and 1970s had the year 2000 in their sights. As we pass "peak Blade Runner" and approach our own landmark year of 2020, technocentric foresight appears to be more pertinent than ever before.

9 Helmer (1967) 12

10 Kahn & Wiener (1967) 87

11 Cornish in Martino (1972) viii

2. How We Did It

Project 2020 elaborated a single world from multiple perspectives. To limit the scope of what otherwise could have been an endless endeavor to map all potential uncertainties, we worked instead to a number of stated and unstated assumptions. As we noted in the white paper, two of these assumptions were that; in 2020 mobile wireless internet would be globally available, "regardless of its divisions; second, persistence of the current dynamic in which technology and the market economy lead where geopolitics and legislation follow."

With the benefit of hindsight we would add a couple of unstated but evident assumptions; the first being that people will continue to do bad things to other people and things using the technology available to them. The second—and by no means less important—that cybersecurity is the responsibility of everyone in society. This last assumption directly influenced our decision to develop scenario narratives from the perspectives of a citizen, a small-to-medium-sized enterprise (SME), a large corporation, and a government. In this respect, our aim of engaging a range of cybersecurity stakeholders determined to some degree how the scenarios looked.

It is debatable whether our first assumption stands up to scrutiny. While it is fair to say that; in 2020 mobile wireless internet connectivity is indeed globally available, it is certainly not pervasive. In many countries where it is available, the cost of data constrains access.[12] As we move forward into subsequent sections of this paper, we will look at the relevance of the issues we raised in 2012 to the real world of 2020. While we are reminded time and again by futures theorists that scenarios are not linear predictions but possibilities, it is nevertheless tempting—and arguably a useful exercise—to identify what we got "right" and what we got "wrong". It turns out that it is fun too.

[12] See for example this recent article by the BBC: "Congo student: 'I skip meals to buy online data'" - https://www.bbc.co.uk/news/world-africa-50516888

3. How Did We Do?

For each of the narratives, we highlighted key technological features of the world in 2020 and how these enabled the activities depicted in the scenarios. For example, for our individual citizen, named Kinuko, these were:

- Augmented reality and highly personalized 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

Review of each of these features against media coverage and other open source material reveals the following:

	Feature	Present in 2020	Mainstream in 2020
Citizen	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	✓	✓
Business	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		
Government	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, havens for cybercriminals	✓	
	Increasing tensions between governments and multinational 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	✓	✓

Figure 1. Features of the world, Project 2020 vs. actual 2020

All features, except a dedicated internet for secure payments, can be said to be present to some degree in 2019/2020. In the act of reviewing, however, it rapidly becomes evident that, in addition to identifying whether a particular technology or threat is present, it is necessary to differentiate to what extent it is mainstream or typical of life in 2020. We are immediately presented with the challenge of determining an objective measure of what is mainstream. Mainstream to one individual in a particular location or milieu may not be mainstream to someone in another.

Regarding a dedicated Internet for secure payments, we have indeed moved closer towards a splinternet, but one of a different order. In the scenarios, we referred explicitly to attempts by some countries to impose national sovereignty on the internet. We were somewhat optimistic in envisaging that an "International Treaty for Cyberspace" would have been concluded and an "International Cybercriminal Court" established by now. But while in the last eight years many nation states have arguably become increasingly entrenched in their approaches to cybersecurity and even to the content permissible online, the UN's recent establishment of an Open Ended Working Group on "Developments in the field of information and telecommunications in the context of international security" and the Paris Call for Trust and Security in Cyberspace may be taken as indicative of a desire for greater international consensus.

Financial institutions, meanwhile, have made greater investments in cybersecurity, increasing the capacity of their in-house information security functions and deploying several iterations of two-factor authentication for their customers. While the industry is working towards mandatory universal payment confirmations by the end of 2020 for the SWIFT messaging system (target of APT 38 and the Banswift and Odinaff malware in 2015 and 2016), the advent of open banking as provided for under the Revised Directive of Payment Services (PSD2) has given rise to new risks to open APIs and FinTech providers, as highlighted by Trend Micro Research.[13]

[13] https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/unlocking-payment-confirmations/why-confirmations_; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2

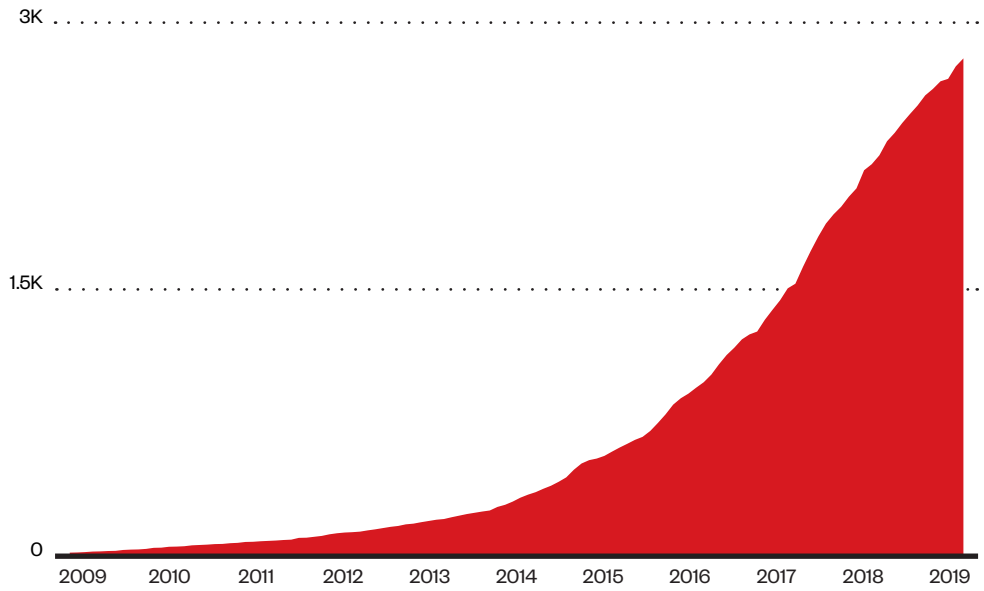


Figure 2. Growth trend of a subset of financial sector API hostnames, taken from Trend Micro™ Smart Protection Network™ (SPN)[14]

For at least two of the envisaged developments the outcome is less certain. The extent to which countries with lower levels of cybersecurity have become "no-go" areas and havens for cybercriminals is difficult to quantify without further research. At a cursory level, one can observe that countries among the lowest ranking in the International Telecommunication Union's Global Cybersecurity Index also tend to be those that are either subject to disproportionate misuse of their country code top-level web domains (some island nations) or are sources of heightened cybercriminal activity.[15] Trend Micro's ongoing research into regional and national variations in cybercriminal behavior[16] uncovers cultural differences in methodology, TTPs, and criminal cooperation, but more detailed assessment is required to determine to what degree this has resulted in large scale "jurisdiction shopping".

An additional question mark hangs over whether attacks on critical information infrastructure resulting in physical destruction and violence have become mainstream events. In the years since 2012 we have witnessed attacks that left countries without power supply, and targeted nuclear power stations or the safety systems of petrochemical companies.[17] Trend Micro Research has conducted several honey pot-based experiments[18] that confirm that malicious actors are actively scanning for and

[14] Ibid

[15] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[16] https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground-economy-series

[17] https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/; https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[18] https://blog.trendmicro.com/trendlabs-security-intelligence/whos-really-attacking-your-ics-devices/; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-gaspot-experiment; https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot; https://documents.trendmicro.com/assets/white_papers/wp-exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.pdf

compromising industrial targets with levels of sophistication varying from curiosity, through opportunistic to highly professional.

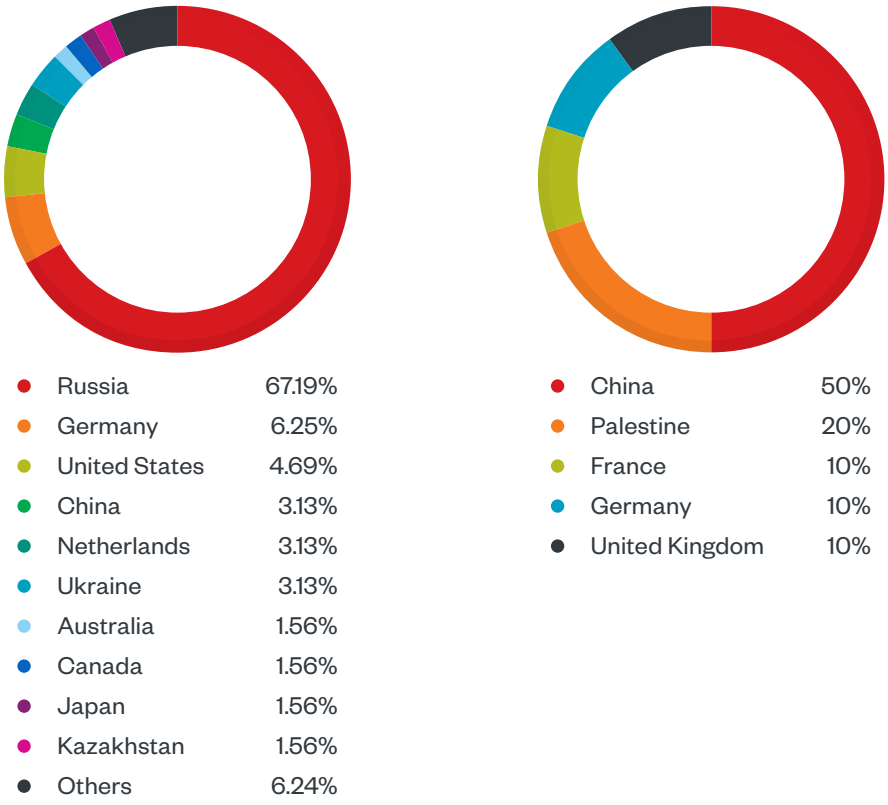


Figure 3. Breakdown of origin countries for non-critical (left) and critical (right) attacks from Trend Micro SCADA honeypot research in 2013[19]

Meanwhile, indiscriminate distribution of ransomware variants including Wannacry, NotPetya and LockerGoga has impacted on healthcare provision, international logistics and heavy industry.[20] Over the course of the decade the ransomware distribution model has moved steadily from "indiscriminate" to highly targeted. Trend Micro's 2019 Annual Security Roundup[21]details a continuing trend where a greater number of ransomware related events were detected even though the number of new ransomware families continues to be in steep decline. One possible conclusion from this disparity is that the amateur players have moved on from ransomware as a threat model due to diminishing returns from low-level crime. The more professional attackers continue to use ransomware in highly-targeted attacks against corporate entities where the financial demands can be orders of magnitude greater than in a successful attack against an average consumer.

[19] https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-scada-that-didnt-cry-wolf.pdf

[20] https://www.nature.com/articles/s41746-019-0161-6.pdf; https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[21] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats

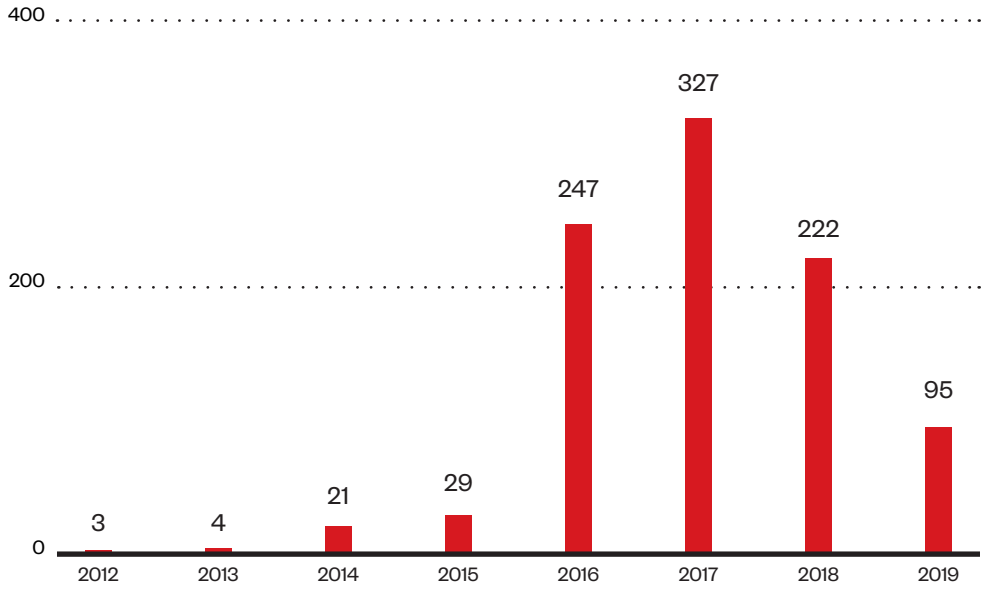


Figure 4. Number of new ransomware families seen throughout the years[22]

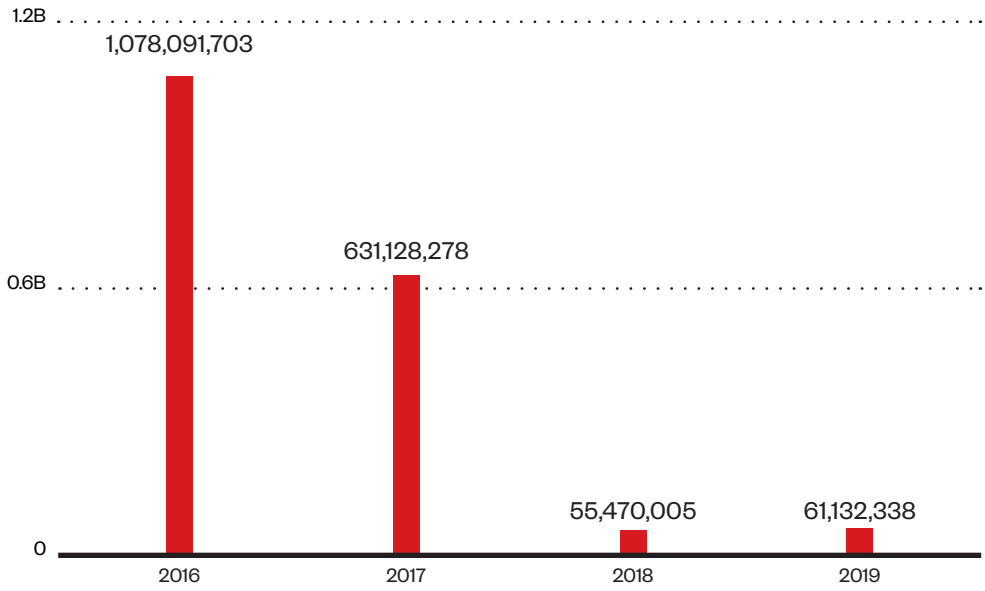


Figure 5. Number of ransomware-related threats blocked[23]

[22] https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf; https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/magnified-losses-amplified-need-for-cyber-attack-preparedness; https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/setting-the-stage-landscape-shifts-dictate-future-threat-response-strategies; https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2016-roundup-record-year-enterprise-threats; https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-annual-roundup-the-paradox-of-cyberthreats; https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unraveling-the-tangle-of-old-and-new-threats; https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats

[23] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unraveling-the-tangle-of-old-and-new-threats

2018		2019	
Manufacturing	1,195,372	Manufacturing	789,455
Government	621,166	Government	585,561
Education	534,954	Education	494,059
Healthcare	403,974	Healthcare	360,954
Technology	304,429	Financial	269,551
Energy	167,977	Technology	222,253
Telecommunications	157,096	Energy	165,466
Oil and Gas	144,762	Telecommunications	141,223
Financial	135,644	Oil and Gas	117,048
Retail	99,657	Food and beverage	112,019

Figure 6. Top identified industries affected by ransomware in 2018 and 2019

One recent study of cyber attacks on operational technology—defined as including energy and utilities, health and pharmaceuticals, industrial and manufacturing, and transportation—reported that 33% of organizations in the sector had experienced an attack that had caused significant downtime in the last 24 months.[24] A Trend Micro white paper in 2018[25] demonstrated that even a snapshot of the internet-accessible attack surface of the water and energy industries offers ample scope for malfeasance. It is therefore reasonable to assume that a large number of attacks with an impact on critical infrastructure do not come to public attention and that at least some of these have led to physical destruction or violence towards people or things. But since this number is uncertain, we cannot know how mainstream an occurrence they are.

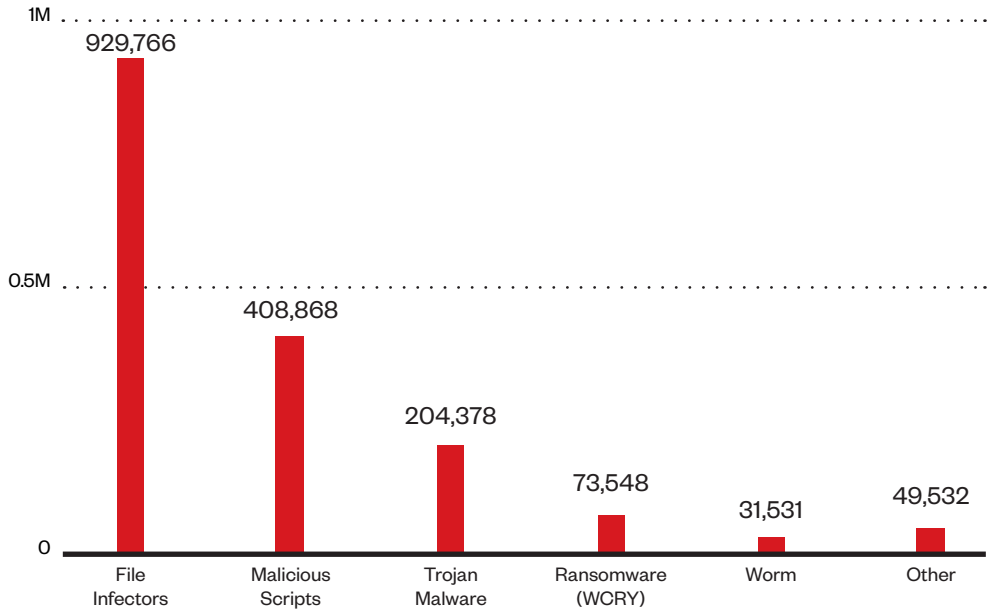


Figure 7. Type breakdown of the top 20 malware affecting organizations in the water and energy industry (October 2017 to February 2018)[26]

[24] https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report

[25] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries

[26] Ibid.

Looking back from the vantage point of 2020, the general questions we raised for decision makers in 2012 remain pertinent:

- 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?

The key considerations for 2020, namely:

- Intellectual property
- Data protection and privacy
- Identity and reputation
- Internet governance
- Tensions between corporate entities and governments
- Risk-based vs. control-based cybersecurity models

The above are also reassuringly relevant. Let us take some of these key themes in turn.

Intellectual Property and New Business Models

In 2012, we were starting to see the Creative Commons movement gain in popularity. Since then, we have seen Facebook make a large number of its tools open source, Tesla make its electric vehicle patents freely available, and Google and eight others—including Samsung, LG, and HTC agree to share patents covering Android™ and Google apps.[27] For these large technology companies, at least, the business model no longer relies on the exertion of absolute intellectual property (IP) rights. Rather, the industry increasingly open sources some of this IP to app developers and others, thereby fostering the explosion of the app market and opening up a new arena of work for the technically minded.

As the era of user generated content reaches maturity, we have new tensions, especially with respect to audio-visual rights. Music streaming has challenged traditional business models and acts have had to adapt. Some have chosen to exert

[27] https://opensource.facebook.com/; https://www.tesla.com/en_GB/blog/all-our-patent-are-belong-you; https://www.theverge.com/2017/4/3/15164556/pax-google-samsung-htc-lg-patent-peace-group

their rights against the likes of Spotify (think Taylor Swift), others have shifted their focus to generating revenue through touring, still others use dedicated software and seek to enforce against ordinary citizens sharing copyrighted content on social media. The phenomenon of reaction videos has tested the notion of "fair use" of copyrighted material, with some rights holders demanding removal of content or compensation for non-payment of royalties.

At the same time, many people have been able to turn their hobbies into careers, enabled by social and broadcast technologies. The YouTuber beauty experts, the Instagram influencers, the small businesses operating entirely on Facebook or Etsy; all of them are challenging the notion that workers do the same thing for eight hours a day in an office or factory. In our scenarios, Kinuko is depicted as a maker and as a fully-fledged member of the gig economy, five years before the term was popularized. And while Kinuko's work is more visibly creative than that of the average Amazon or Uber driver, it nevertheless reflects the possibilities we saw in 2012 for a larger number of people to have portfolio careers.

Data Protection and Privacy

When we built the scenarios in 2012 there was a certain amount of hype around an emerging trend for lifelogging. A tiny camera with a then-impressive 5 megapixels was generating enthusiasm in the tech press.[28] Since then, of course, the camera has become an increasingly important feature of our phones. Device manufacturers have invested heavily in improving camera quality, spurred on by the public's urge to share on social media. We have also seen the emergence of the "quantified self", including fitness, sleep and health tracking, consumer DNA profiling and, perhaps inevitably, breaches of this very personal data. While in *Project 2020* we consciously stopped short of directly depicting the potentially distressing consequences of misuse of this kind of data on one of our main characters, the world we described was one in which terrorist attacks on data centers had resulted in elderly people falling seriously ill, and this vulnerability was suggested by the dependence of Kinuko's great-grandfather on remote monitoring.

We foresaw that greater collection of data in relation to our personal movements and daily activities would create new data profiling possibilities, new legal questions, and new security risks. In the intervening years, we have seen concerns expressed and legal action over the aggregation of data from different services by large tech companies, particularly where sensitive medical or fitness data forms part of the proposed bucket. We have seen the mass adoption of contactless payments for travel and retail, and the deployment of facial recognition for security and public order purposes. Technology

[28] https://www.theverge.com/2012/10/23/3539986/memoto-camera-lifelogging-kickstarter

companies and government authorities have more access to data about our lifestyles than ever before. This has prompted moves to develop alternative models that give control back to the data subject, Tim Berners-Lee's company Solid among them.[29] In response to high-profile data breaches and apparent privacy concerns, end-to-end encryption is increasingly the default standard for messaging. Once the preserve of security specialists, activists and criminals, VPNs are now being marketed on TV. Privacy protection has gone mainstream.

Accordingly, we have seen new regulation, which answers a number of the questions we posed to cybersecurity stakeholders in the *Project 2020* white paper. The EU's General Data Protection Regulation (GDPR) defines the roles and responsibilities of data controllers, processors, and subjects[30], imposes response requirements and penalties for data loss, and helps to clarify the distinction between legitimate use of data and its misuse. Several high-profile cases have highlighted how challenging the last of these can be. The Cambridge Analytica scandal revealed the extent to which data shared for one purpose (a social personality test) could be subject to unauthorized sharing on a grand scale for quite another, that of political advertising. On the issue of surveillance, the reported activities of HackingTeam, NSO Group, and others have drawn attention to the alleged use of commercial intrusion capabilities by a number of governments, and the rise of stalkerware has prompted the US Federal Trade Commission to ban a number of apps.[31]

Identity and Reputation

In 2012, we could already see that the notion of identity was in flux. Since then, many ordinary citizens have adopted multiple online personae, using different usernames and access credentials for different services. A move towards cloud-based enterprise operations has prompted many cybersecurity providers to add Identity and Access Management (IAM) to their offerings.

During the same period, public and media interest in cybersecurity incidents has grown, with the result that they now have greater reputational impact than in 2012. One recent study observed that "cyber breaches" can wipe as much as 15% off a company's value, and that share prices fall by an average of 1.8% on a permanent basis following a severe breach.[32] Another found that, of 28 companies listed on the New York Stock Exchange, average share price was still down against the NASDAQ by -13.27% three years after a publicly disclosed breach of 1 million or more records.[33] When we

[29] https://solid.inrupt.com/how-it-works

[30] https://www.trendmicro.com/en_us/business/capabilities/solutions-for/gdpr-compliance/gdpr-resource-center.html

[31] https://www.technologyreview.com/f/614614/the-ftc-has-banned-a-company-from-selling-stalkerware-for-the-first-time/

[32] https://www.cgi-group.co.uk/en-gb/white-paper/cyber-value-connection

[33] https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/#Long_term_effects_of_data_breach_on_share_price

were building the scenarios we noted an emerging market for outsourcing corporate online reputation management as a possible signal for the future development of the rise of a new identity management industry. Communications and public relations agencies have evolved accordingly and increasingly we have seen organizations of all sizes build out digital engagement and social media functions, and include crisis communications in their cyber attack and data breach response plans.

Corporate information security has also become a matter of national reputation and security. The very public debate surrounding the inclusion of Huawei products in several nations' 5G infrastructures illustrates the extent to which distinctions have blurred between cybersecurity and national security, and—as we highlighted in the white paper—between internet diplomacy and international diplomacy. Cyber attacks have also combined with disinformation campaigns to negatively impact on the reputations of individual politicians, thereby interfering in democratic process and the rule of law.

Internet governance, tensions between corporate entities and governments

In the scenarios, we envisaged a continuation of the multi-stakeholder internet governance model observable in 2012. Our fictional Internet Authority bears more than a passing resemblance to IANA, ICANN, the Internet Engineering Task Force (IETF), and the Internet Governance Forum (IGF). We described it as "a coalition of the willing", and cautioned that a lack of unity in internet governance would mean a lack of unity in cybersecurity. [34]

In 2020, internet governance remains a matter of multi-stakeholder cooperation. At a national level, cybersecurity continues to be a cross-sector endeavor; the landscape of Computer Emergency Response Teams is a patchwork of government, industry, and civil society entities. The IETF draws on voluntary membership in its work on, for example, standardizing protocols for the Internet of Things, and on network issues related to the realization of AR and VR.

While consensus remains the dominant model, national approaches to internet governance and cybersecurity pose a growing challenge to international interoperability.[35] Flexing of national sovereignty in relation to internet infrastructure, domestic isolation exercises, data localization requirements and surveillance and content restriction signal further Balkanization.

[34] https://www.intgovforum.org/multilingual/filedepot_download/9212/1804

[35] https://www.trendmicro.com/vinfo/ph/security/news/online-privacy/why-internet-routing-affects-digital-sovereignty

Counter to this runs the grouping of citizens into global communities on social media, and in environmental and political movements. In the white paper we remarked how in 2012 these global networks of citizens were already challenging corporate and government interests. We suggested that by 2020, they could well be a powerful force in cybersecurity. Since then, non-profits in North America, Europe, and elsewhere have held tech companies to account for their data transfer practices and compliance with legal requests and have publicly challenged national laws on surveillance and online content. Meanwhile, the existential opposition between online services with global communities and global terms of service on the one hand, and national laws and customs on the other, has resulted in an apparent stand-off between governments and Big Tech.

Risk-based vs. control-based cybersecurity models

The white paper highlighted a key tension between risk-based and control-based approaches to cybersecurity. We associated control models with security through lockdown, heavy reliance on technical prevention, internet filtering, absolute protection for intellectual property, and suboptimal interoperability. Risk-based approaches, on the other hand, were 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. We envisaged that 2020 would exhibit a combination of the two. At a strategic level, this is reflected in the aforementioned patchwork of approaches to intellectual property, Balkanization, and the flexing of national sovereignty. At the same time, the entry into force in 2019 of the EU Cybersecurity Act has introduced a framework for EU-wide cybersecurity certification, thereby giving businesses the opportunity to provide greater security assurance for their products, services, and processes.[36]

At the operational level physical, procedural, and technical controls naturally remain important components of cybersecurity. Role-based access control continues to be a key feature of most organizational approaches, following the principle of "least privilege" for access to data and networked systems. In line with greater focus on the reputational impact of cyber attacks, we have also seen the rise of corporate cyber risk profiling and the mainstreaming of cyber risk insurance.

Cybersecurity providers now offer bespoke threat intelligence, including dark web monitoring—the rationale being that the more relevant the information is on the threats posed to an organization, the more targeted and effective the preventive controls and incident response will be. Data mapping exercises required for compliance with GDPR have in many cases assisted in this profiling. An increasing number of small

[36] Regulation (EU) 2019/881 of April 17, 2019) - https://eur-lex.europa.eu/eli/reg/2019/881/oj

and medium-sized enterprises outsources its incident response functions, and there is now a burgeoning market for external security operations centers (SOCs). Our suggestion that "countries and corporations opting for more of a risk-based model are going to need more lawyers, more insurance, and more cybercrime specialists" appears to have been borne out.

We grouped the cybercriminal threats envisaged in the scenarios into categories, which we highlighted in the discussion of implications for cybersecurity stakeholders. These were:

- 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 specific crimes and threats we envisaged are listed in the chart below:

Threats/Activities	Present in 2020	Mainstream in 2020
A market for scramblers of mood recognition, remote presence, and near-field communication (NFC) technologies	✓	
Highly distributed denial-of-service (DoS) 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 centers 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.)		

Figure 8. Envisaged cybercrimes vs. presence and mainstreaming in 2020

Findings of note:

- The overwhelming majority of threats envisaged in the scenarios are present in some form in 2020. As with the world features listed in Figure 1, quantifying the extent to which they have become mainstream has proved more challenging.
- As this review relies on publicly available information, we may need to resign ourselves to the fact that in some cases we simply do not know how frequent certain crimes are in 2020. With regard to physical attacks on data centers and internet exchanges, we can point to the 2018 theft of Bitcoin mining servers in Iceland.[37] Ideologically motivated destruction of hardware is more difficult to identify, and may well be underreported. Related incidents such as criminal damage and security threats at tech company offices, and an increase in popular protests on environmental and social justice issues, may serve as signals for the further evolution of an offline movement against Big Tech, especially its environmental and social impacts.
- When we envisaged cyber-enabled violence against individuals and malware for humans, we particularly had in mind potential for misuse of recently identified vulnerabilities in implantable medical devices. Further issues identified since 2012 have resulted in large-scale recalls and the publication of advisory notices by the US Department of Homeland Security.[38] As in the case of hacks against connected devices, however, there is insufficient public evidence to determine whether these vulnerabilities have resulted in physical harm to individuals. It is possible to assert, of course, that the impact of Wannacry on the UK National Health Service makes this an instance in which malware affected the health of citizens. But what has become more apparent in recent years is the extent to which misuse of internet mediated services has resulted in emotional and psychological harm, with potential physical consequences. The aforementioned stalkerware and documented suicides following sextortion are testament to this. The unwitting exposure of locations of military bases through generation of fitness tracker heat maps highlights the potential for data to endanger physical safety. Meanwhile, the phrase “malware for humans” is now used to refer to the phenomena of fake news and influence operations.
- On the issue of cyber gang warfare we were inspired in 2012 by identified efforts of cybercriminal groups to undermine the operations of their rivals, and apparent “tit for tat” attacks between pro-Israel and pro-Palestine

[37] https://www.wired.co.uk/article/cryptocurrency-iceland-economy-bitcoin-data-centres

[38] https://www.wired.com/story/pacemaker-hack-malware-black-hat/; https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update; https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

groups.[39] Since then, the political aspect of cyber gang activity has increased in importance, with the rise of state-sponsored cyber militias and ongoing activities by, for example, pro-India and pro-Pakistan groups.[40] The reported exploitation of Iranian APT infrastructure by the Russia-based Turla group provides some of the best evidence of continued efforts to compromise the activities of rival criminal groups.[41]

- The misuse of augmented reality for attacks and frauds based on social engineering was predicated on the mainstream adoption of AR technology. This will be discussed in greater detail in the next section.

"Misses"

Heads-up displays

Augmented Reality (AR) was a feature of the narrative for our citizen, Kinuko. This was envisaged as delivered through a Heads-up display (HUD) unit akin to Google Glass, about which there was a good deal of hype in 2012. In the scenarios, AR contact lenses were also increasingly mainstream.

While Google Glass has a number of enterprise users in 2020[42], it has so far failed to live up to its earlier consumer promise. Reported incidents in 2013 and 2014—including a driver being fined for wearing Glass behind the wheel, and an individual being assaulted for wearing Glass in a bar—epitomized the privacy and safety concerns associated with consumer use of the technology.[43] Companies involved in AR development have had to regroup and rethink. Smart contact lenses are indeed of interest to Big Tech, with Google, Sony, Samsung, and Magic Leap all having filed patents for lenses that record video or display augmented content. Mojo Vision's offering was one of the most covered and coveted products at 2020's CES.[44] Glasses, too, may well be making a comeback, if current excitement over NReal's technology is anything to go by.[45] Until now, consumer AR has been a device-based, "heads down" experience, as evidenced by the millions of us who look at our phones while walking or driving through city streets. Whether these people are any safer than they would be wearing HUDs is a question perhaps worthy of further consideration.

---

39 https://arstechnica.com/information-technology/2012/01/israeli-and-palestinian-hackers-trade-ddos-attacks-in-rising-cyber-gang-war/

40 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf

41 https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims

42 https://www.google.com/glass/start/

43 https://www.fastcompany.com/3020899/california-driver-gets-a-ticket-for-wearing-google-glass-behind-the-wheel; https://mashable.com/2014/02/26/google-glass-assault/?europe=true

44 https://www.cnet.com/news/a-single-contact-lens-could-give-your-entire-life-a-head-up-display/

45 https://www.bbc.co.uk/news/technology-51057941

Did we miss AI?

The phrase “artificial intelligence” (AI) is the most obvious omission from the scenario narratives. Machine learning is very present: Kinuko’s behavioral data is used “to teach computers how to be more human”, she makes use of live language translation when on a VoIP date with someone from Mexico, the components used by assemblage SME Xinesys are able to make intelligent decisions about their transport. But we did not call out AI specifically, or anticipate the degree to which it would come to dominate technological discourse by the end of the decade. Consideration of why that may be the case inevitably challenges us to review the emergence of AI in recent years, and to reassess industry and scientific material from 2012. It is perhaps of note that AI did not feature as a distinct category in the Gartner® Hype Cycle for Emerging Technologies for that year:

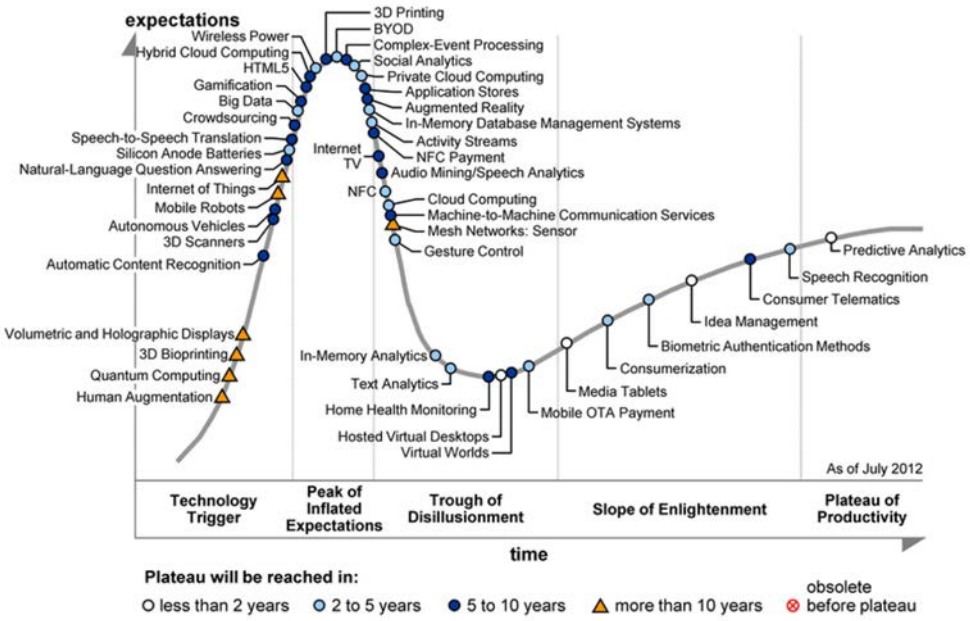


Figure 9. Gartner Hype Cycle for Emerging Technologies 2012[46]

Technologies such as automatic content recognition, natural-language question answering, speech-to-speech translation, and others on this chart arguably would now be branded as AI. Accordingly, Gartner’s Hype Cycle for 2019 includes categories such as “Edge AI” (device-based), “Explainable AI”, and “AI PaaS” (Platform as a Service). What happened in the intervening years? If we query the patent database of the World Intellectual Property Office, we find that abstracts containing the phrase “artificial intelligence” were not subject to a sustained increase until after 2014. By far the largest year on year increase was seen in 2018, with 71% more patents that explicitly referred to AI being filed than in the previous year. Since the number of patents reflects the technologies in development, it is evident that the signals for AI

[46] https://www.gartner.com/en/documents/2100915/hype-cycle-for-emerging-technologies-2012

development were considerably weaker in 2012, and it is therefore understandable that they did not feature more prominently in the *Project 2020* scenarios. This prompts the question whether better use could be made of weak signals in futures exercises. It should also serve as a useful prompt for us to reflect on whether "artificial intelligence" is not so much a discrete technology, as a field of study that is currently giving rise to a number of technological advances, including in machine learning.

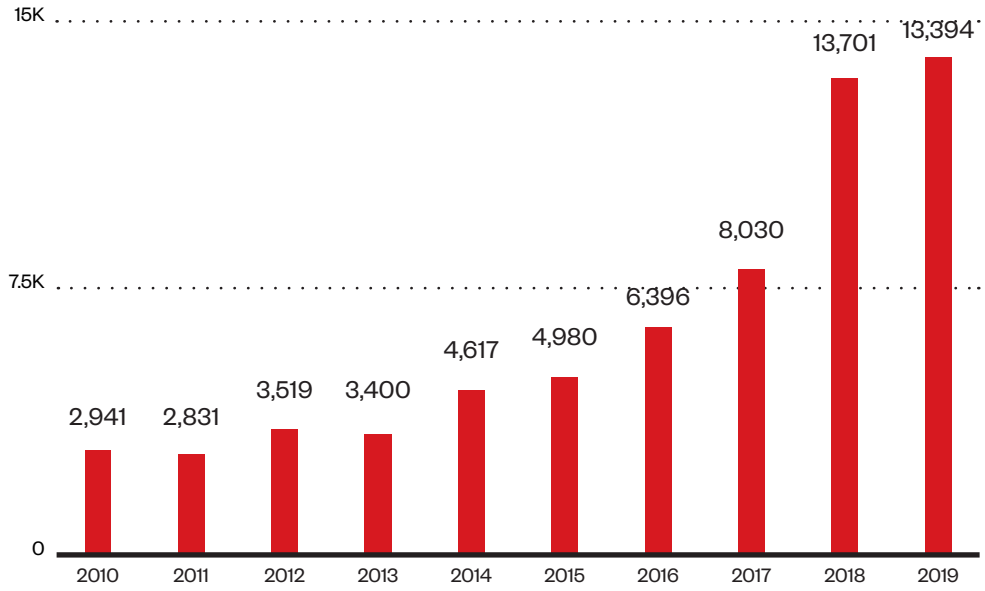


Figure 10. Patent abstracts containing the complete phrase "artificial intelligence", by year filed with the World Intellectual Property Office[47]

[47] Data extracted 29/09/19

4. Landing the Message - Transformation from White Paper to Visuals

The white paper "Project 2020 – Scenarios for the Future of Cybercrime" was published on the Europol and ICSPA websites on September 25, 2013. While it is impossible to ascertain the total number of times the white paper has been read, or the extent to which it has been used, analysis of citations in other publications may provide some indication of the research community's level of engagement with the scenarios. Searches in Google Scholar™ for the strings '"Project 2020"+cybercrime' and '"Project 2020"+ICSPA' reveals citations in five books, all in the subject area of cybercrime, and 34 research and reference articles in the subject areas of cybercrime and futures thinking.[48] This would suggest that the impact of the white paper was largely restricted to specialist audiences.

A number of researchers have cautioned against futures thinking becoming an elite practice, among them Arthur Waskow in the 1970s,: "In an era of very swift technological change, it has to be possible for the whole public to be able to understand the possible futures confronting their society 20, 25, 30 years from now."[49] Recognizing that the white paper had identified all members of society as cybersecurity stakeholders, there was a need to translate the scenarios into something more generally accessible.

Trend Micro took the decision to develop a web-series of nine short live action movies set in the world envisaged in the scenarios.[50] Viewed more than a quarter of a million times on YouTube, the movies were jointly produced by Trend Micro and Black Rabbit Productions in Warsaw, Poland. The release of the series' trailer coincided with the publication of the white paper on the occasion of the inaugural Europol-INTERPOL

[48] Duplicate results were removed from these numbers.

[49] Waskow in Martino (1972) 104

[50] http://2020.trendmicro.com/

Cybercrime Conference. Subsequent episodes and a "making of" clip were released over a period of two months, the final instalment airing on November 26th 2013. Additional collateral, including 2020-themed wallpapers for desktops and mobile devices, was made available for download from a dedicated website. The main reason for the translation from white paper to web series was to engage with a wider audience than the "already interested". We envisaged the video material as a conversation starter in educational establishments and commercial organizations alike as we attempted to bring to life many aspects of the world only glimpsed in the white paper. During this three month campaign, Trend Micro's US Twitter, Facebook, Google+, LinkedIn, and YouTube profiles alone generated 687,575 organic impressions for 2020 content and experienced a 41% total increase in audience size. The Trend Micro YouTube channel, where the videos were uploaded, received a 66% increase in subscribers due to the campaign, as well as an 862% increase in average engagement per video. The series also resulted in national news coverage in USA Today[51] among many others and was nominated for many international awards and won several of them including a nomination in the Shorty Awards, the World Media Festival in Hamburg 2014 (Grand Prix, Grand Award; Web and Web TV, Gold Award; Web), Worldfest Houston 2015 (Gold Remi Award; New Media), Webfest Montreal 2015 (People's Choice Award), Accolade Global Film Competition 2015 (Award of Merit), and UK Web Fest 2015 (Best Production).

[51] https://eu.usatoday.com/story/cybertruth/2013/10/07/video-series-depicts-cybercrime-in-2020/2938513/

5. Concluding Thoughts

The review of futures exercises is something that is not often done. The momentum to move on to the next task, challenge or horizon is often too great for us to stop and take stock. But doing so not only gives us the opportunity to improve our methodology. It also allows us to pause and consider how we got here, to trace developments in the intervening years.

In methodological terms, *Project 2020* presents scenarios in the broadest sense as defined by Shell International: "A scenario is a story that describes a possible future."[52] The project departed from the standard scenario technique of building alternative possible futures for further consideration, opting instead to depict one possible future from several perspectives, with technology as the single independent variable. We also chose a shorter timeline than most scenario exercises, reflecting the accelerative effect of technology identified by earlier futures thinkers. What emerges is an approach that is somewhere between a forecast and scenarios—"short range scenarios" if you will. Introducing a limited Delphi-style review at two stages in the project increased the likelihood of plausibility in the scenario narratives. It also confirmed the project's methodology as something of a hybrid.

In considering the success of the project in terms of what we "predicted correctly", we are also guilty of letting ourselves be dragged into the business of treating scenario narratives as linear forecasts, when they are intended to be anything but. In reviewing, we have taken heart from the fact that even the best resourced (Gartner) and most learned/best informed (Helmer) get some of these things wrong. When we consider also that Blade Runner's screenwriters were compelled to shift their horizon to 2019 from Dick's original date of 1985, we may count ourselves in good company.

[52] Shell International (2008) 8

Nevertheless, the fact remains that the overwhelming majority of key questions and implications identified in the Project 2020 white paper are relevant today. The same goes for the specific criminal activities and cyber threats envisaged. While measuring their extent and impact has proved challenging, they are certainly present. Where we missed the mark, this has enabled us to identify additional factors for inclusion in subsequent exercises.

There are obvious limitations to this review, chief among them the fact that it is not independent. While directly involved in building the scenarios and drafting the narratives, we have endeavored to conduct an objective and rigorous review with the aim of finding ways to optimize both the methodology and the outcomes of cybersecurity futures exercises.

Project 2020 was destined to be an unusual exercise in so far as the scenario narratives were drafted with the entirety of society as their intended audience. This was reflected in the subsequent web series of movies. There may be further opportunities to measure public engagement with the content via social media polling. Moreover, futures exercises conducted in 2020 now have a plethora of social engagement and measurement tools at their disposal.

Could we have done *Project 2020* differently? Absolutely. With limitless financial, technical, and human resources, we could have analyzed all the information available, asked all the experts, and come up with scenario narratives that were exhaustive. Given the short time frame and relatively small scale of the project, its vision was remarkably prescient. We would need to rerun the exercise to know whether this was a fluke.

Appendix: Further Reading

Amer, M., Daim, T. & Jetter, A. (2013) “A Review of Scenario Planning”. Futures 46: 23-40.

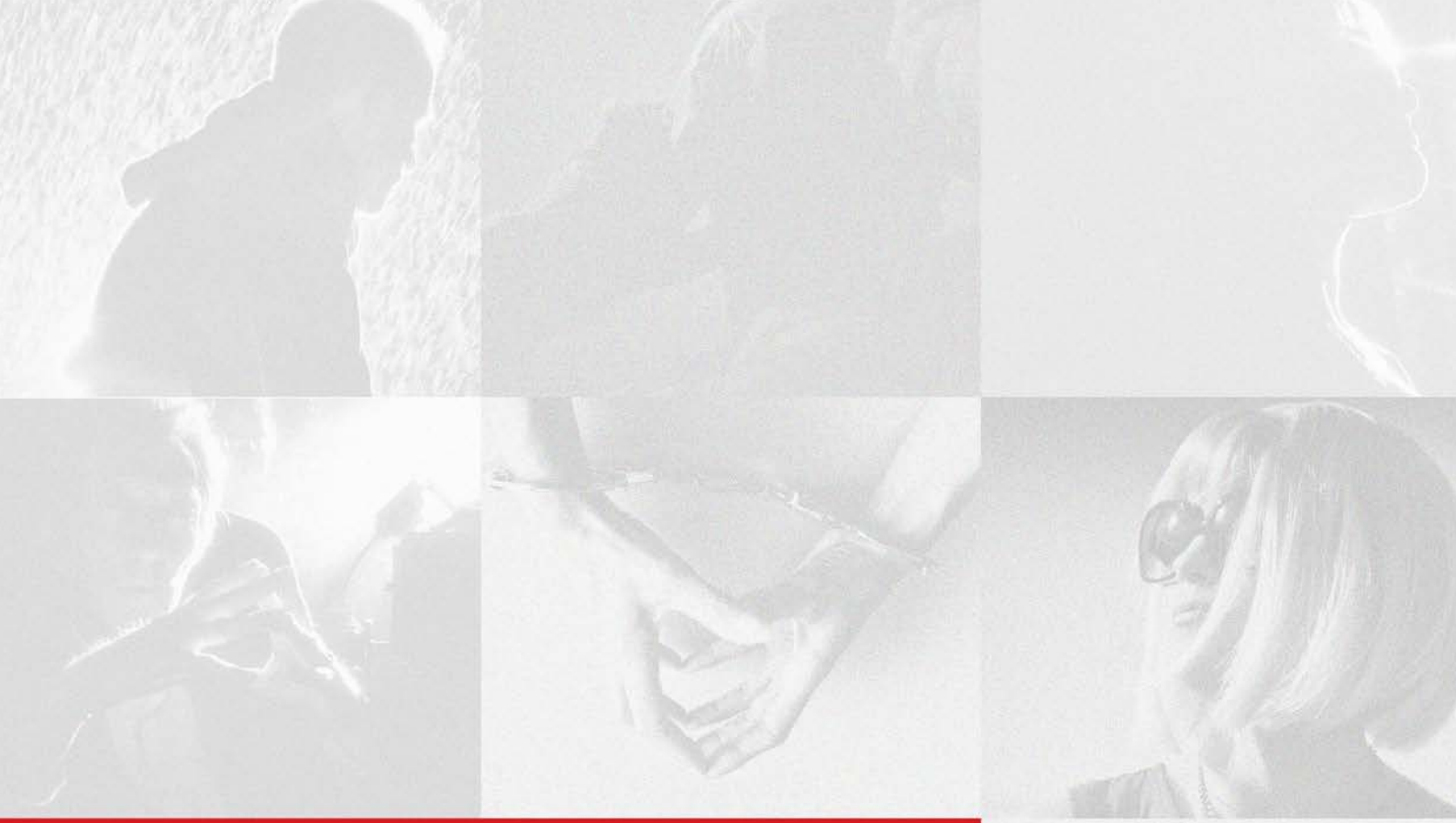
Helmer, O. (1967) *Prospects of Technological Progress.* RAND Corporation. Santa Monica.

Kahn, H. & Wiener, A. (1967) *The Year 2000: A Framework for Speculation on the Next Thirty-Three Years. Macmillan.* London.

Martino, J. ed. (1972) *An Introduction to Technological Forecasting. Gordon and Breach.* New York.

Shell International (2008) *Scenarios: An Explorer’s Guide.* The Hague.

Toffler, A. (1970) *Future Shock.* Pan. London.



TREND MICRO™

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™

Securing Your
Connected World