Tomorrow's Internet

Summary: The Internet is poised to change in multiple, potentially radical ways. New regulatory frameworks could significantly alter expectations for data security, and potentially transform the business models driving major Internet companies. The Internet's physical infrastructure is also changing rapidly, with growth of the Internet of Things moving objects in the physical environment onto the Internet and creating significant new security challenges.

Forecasts

- The Internet of things will bring billions of devices onto the Internet, blurring the boundaries between physical and digital threats. Balancing the competing needs for efficiency, compatibility, and security will be a key challenge for tomorrow's Internet.
- National Internet-related regulations, such as a GDPR in the EU and the "Great Firewall" of China, will proliferate. Global companies will increasingly need to create local adaptions of their services to comply with new national or regional regulations.
- Human users will engage with the Internet in new ways, using voice interfaces and AI assistants, or interacting in the data-enhanced environments of augmented reality and virtual reality.
- Over the next decade most new Internet users will come from emerging or underdeveloped countries, accessing the Internet primarily through their mobile phones. This will accelerate the shift towards smartphones and apps being a primary gateway for Internet access.

Key uncertainties for the future of the Internet:

- Enactment of new Internet regulations by various countries around the world
- Impact of new technologies on whether hackers or defenders have the advantage on digital platforms
- Extent to which national governments exert control over Internet companies
- Role of blockchain technology in future Internet infrastructures
- Ability of new decentralized Internet services to disrupt current industry leaders

Supporting trends

Internet of Things. The Internet of Things (IoT) is the next wave of Internet development, extending Internet connectivity and interaction to billions of objects and devices.

Cognitive computing. Supercomputers for deep learning and AI applications are falling in price and shrinking in size.

Anticipatory ambient intelligence. Ambient intelligence may lead to AI systems anticipating consumers' needs in every aspect of life.

Affective computing. Affective computing integrates emotion detection and simulated psychological sensitivity into computers.

Backlash against major tech firms. Calls to regulate major social-media platforms are growing.

Net non-neutrality. The neutrality of Internet companies is declining for political and business reasons, with many companies taking a more active role in regulating content.

New cloud infrastructure. New approaches to cloud computing are emerging, such as hybrid clouds and serverless clouds.

Consumer-centric bots. Consumer-centric bots help to empower consumers against companies, by using algorithms to cut through bureaucratic complexity.

Voice interfaces getting smarter. Developers are working to take voice interfaces beyond "natural language" to "conversational."

Data points

***Internet for the global south*.** By 2025, some of the poorest areas on Earth will have significant Internet penetration. India's user base is forecast to increase from 400 million in 2017 to 850 million by 2025. Africa will see similar growth over that timeframe. Smartphone use on the continent is projected to increase from 226 million users in 2015 to 720 million in 2020, greatly increasing Internet penetration.

Internet of Things growth. According to International Data Corp, global spending on the Internet of Things (IoT) will increase 14.6 percent in 2018, reaching $772.5 billion during 2018. Spending is projected to reach a trillion dollars annually as soon as 2020.

Topics for additional research

- Emerging decentralized Internet technologies
- IoT security innovations

Strategic insights

For the security industry

- Internet of Things devices are spreading rapidly, and will quickly become ubiquitous in physical environments. Deployment of these technologies will change the nature of digital threats, shifting the impact away from IP protection and towards life-and-death threats to workers or business continuity.
- The security industry will need to adapt to the "information security" paradigm being eclipsed by a new "critical infrastructure" paradigm. This will create new opportunities for cybersecurity professionals to handle issues beyond IT systems. However, other organizational stakeholders will have to be convinced of the extent of the new security challenges.
- Automation and machine learning will add new capabilities to the existing portfolio of cybersecurity threats, as well as create novel threats. Identifying the new vulnerabilities caused by these technologies will become increasingly important for the security profession.

For ASIS

- Information security is converging with other functional areas within organizations, fueling a potential challenge from information security organizations that could plausibly encroach on the domain of traditional security associations. However, the diffusion of information security could also loosen the influence of IT-focused associations and open up new opportunities for non-IT associations.
- AI systems will play a growing role in mediating communications between ASIS and its membership, creating both challenges and opportunities for member engagement.

Timing

- **Stage**: Growing, in a period of technology transition
- **Speed**: Fast, and driven by the most innovative sectors in the economy

Potential alternative futures

- **Internet balkanization.** Nations enact their own approaches to Internet regulation, fracturing the notion of the Internet as a globalized whole.
- **Tech oligarchs.** Competition between tech companies comes down to a handful of giant global companies that have the capability to deal with a complex global regulatory landscape
- **Internet 3.0.** Growth in the Internet of Things boosts demand for more decentralized Internet technologies. New services are able to displace today's tech giants.
- **Appification.** The Internet fades into the background, and younger users come to view it is a mere conduit for their must-have apps and cyber services.