THE NEW INFORMATION ENVIRONMENT
DISCOVERING WHAT MATTERS

MAY 2017

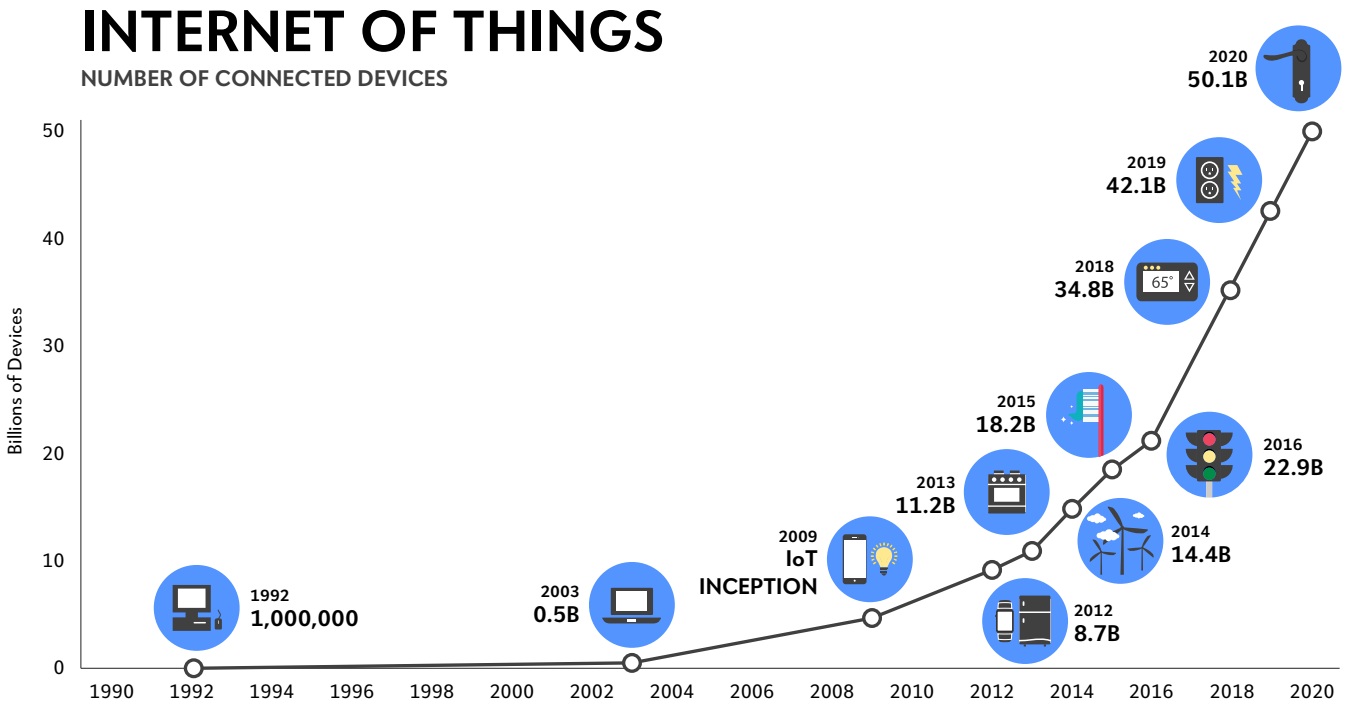
Bottom Line Up Front

The evolution and proliferation of information technologies have fundamentally changed the information environment and disrupted our decision and policy making processes.

The environment has shifted from one in which information was relatively scarce and costly to one in which it is dense, ubiquitous, and cheap. With the rise of the internet and social media, the negligible costs to produce, transmit, broadcast, and consume information has upset established power structures. The challenge for decision and policy makers has gone from gaining access to information, to distilling large amounts of data down to relevant and actionable insights.

While this new environment presents novel opportunities, it also creates a number of challenges including hindering policymaking, impeding effective governance, opening new domains for warfare, and introducing systemic vulnerabilities.

To grapple with the new environment, novel strategies, tools, approaches, and processes are needed.



Source: The Network and Television Association
https://www.ncta.com/positions/internet-of-things

Discussion

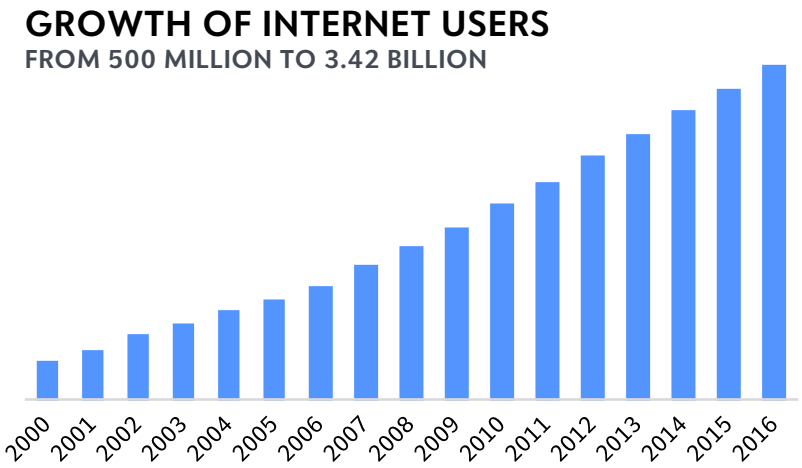
THE EVOLUTION OF INFORMATION

Human-made information derives from our ability to encode knowledge and ideas into various media. The way information is produced, transferred, broadcast, and consumed generates an information environment that individuals and organizations must navigate.

From the invention of spoken language through the digital revolution and the emergence of the internet, all progress has made information travel farther faster, and persist longer, with less manpower. The negligible costs to produce and transfer information near-instantaneously is leading to a massive proliferation of data. Wal-Mart, for example, produces more data every two hours than the amount held in the Library of Congress.

Today, information is no longer limited to human-to-human communication; machines are also active in the information ecosystem. Over half of the activity on the internet is generated by bots and other automated agents. Moreover, objects and infrastructure are increasingly interfacing with the internet, a trend referred to as the "Internet of Things" (IoT). Estimates of the number of devices that will be connected to the internet by 2020 range from the tens to hundreds of billions.

As the capacity and ubiquity of information technologies continue to increase, we are entering a new information environment that both the public and private sectors must grapple with. This new environment and its effects are the primary catalysts for the social and political disequilibrium across the globe that has so far marked the 21st century.



Internet users are now not only the consumers but also the producers of information.

With the proliferation of users and their devices connected to the internet, the amout of data being produced, collected, and shared will only continue to grow.

Source: internetlivestats.com

FROM THE OLD TO THE NEW

The old environment was slow and orderly where information was a scarce commodity. High costs and technological limitations were major obstacles in capturing, storing, and transmitting information. Consequently, a relatively small number of organizations in the form of news media and research firms specialized in these activities, serving as arbiters of valuable information.

The consolidated and centralized nature of these organizations meant that informational flow was easy to control and that consumers of information faced the same information environment due to reliance on common trusted sources. This engendered a shared perspective and understanding of events and the state of the world.

The relevance of available information was generally understood by both providers and consumers. Information was curated only when there was a belief in its utility; irrelevant information did not justify its own costs.

Conditions of scarcity meant that not everyone had access to relevant information. This allowed so-called information asymmetries to be maintained, leading to persistent power structures in business, governance, and warfare. In business, this translated into profit; in governance, the ability to strongly influence the sentiments of the population and political outcomes; and in warfare, victory or defeat.

The new environment is fast and chaotic. The arrival of the internet, mobile devices, and social media has created a glut of information and interconnectivity. High-speed and high-bandwidth infrastructure have made it possible for nearly anyone to transmit dense data streams at a global scale, all but eliminating the persistent competitive advantages of the past. Mobile devices keep individuals and organizations continuously connected.

Traditional media outlets no longer hold a monopoly on the ability to capture and broadcast information and events. An IT consultant in Abbottabad, Pakistan first reported the US military raid against Osama bin Laden in May of 2011 on Twitter. This happened as events were still unfolding on the ground and hours before the American people were officially notified by the President of the United States' address.

People and things that were previously disconnected are now connected and networked. This connectivity affects real-world, physical systems, including those critical for national security. Events whose effects would have dissipated in the old, disconnected environment can now have far reaching consequences. Connectivity also makes the effects of actions difficult to predict by increasing the prevalence of side effects and unintended consequences. Simply, there are more pathways for impacts to travel along, and therefore more ways for things to go wrong. And because information is so cheap to amplify, the size of effects can grow rapidly.

The proliferation of information sources also means that individuals and organizations no longer have a shared information environment. Instead, they must filter and be selective in which variables and stakeholders they attend to. This leads to divergent and often conflicting viewpoints and sets the conditions for social fracturing. Events no longer have self-evident meaning: the exact same events viewed through different frames can have vastly different significance and interpretations.

Because the source of information is often far removed from the consumer, verification has become extremely difficult. Misinformation and disinformation are rampant, leading to a low-trust environment in general, and exacerbating divergences.

In journalism, there is now greater incentive to get things first than to get things right. Stories are rushed to the web, where they can be picked up by other outlets who also seek to beat their competitors to the punch and propagate stories that support their viewpoint. This can lead to a cascade of self-reinforcing information that creates the appearance of a multiple-sourced fact, which may or may not reflect reality.

All of these factors combine to create a crisis of relevance. How can we know what information matters for making a decision, where to find it, and what actions will achieve our aims?

In the new information environment, gaining access to data is no longer the major expense and challenge. Rather, the main challenge now lies in filtering through myriad sources and discovering relevant, reliable, and actionable data. Moving into the future, those with the ability to parse and make sense amidst the noise, and to take swift and effective action, will be the ones with competitive advantage.

CHALLENGES

The new information environment demands that we rethink the way institutions operate to achieve success.

The flood of data and signals means that to succeed, both public and private organizations must develop means of filtering through the noise to discover relevant and actionable insights. Importantly, this means knowing what not to expend resources on. Policymakers must wrestle not only with vast amounts of information, but with its social and political consequences; namely social unrest, fracturing, and political polarization. These dynamics have created a tense environment, promoting hyper-partisanship with little room for compromise.

In our foreign engagements, unprecedented levels of information warfare have created a disorienting environment and sown distrust. Moreover, threats continue to escalate from both state and non-state actors empowered by information technologies. These realities have exposed organizational deficiencies in addressing what will be persistent challenges to national security.

Finally, the proliferation of the "Internet of Things" and growing reliance on interconnected networks introduces systemic vulnerabilities. In particular, the public and private sectors together are facing novel threats to critical infrastructure.

(1) Too Much Information

When information was scarce, there was a pervasive belief that with enough information, we could put the big picture together and take decisive action to succeed.

The proliferation of information has led to the exact opposite situation; our vision has never been less clear. We are doing more and understanding less. Networks of cause and effect bound together by digital information have become nearly impossible to decompose and understand; we now

have more data than insights. This has led to a state of extreme uncertainty with regards to what actually matters and the potential consequences of any given actions in an increasingly complex and interconnected environment.

Data Unit	What it means
Byte (B)	1 Byte: a single letter or number
Kilobyte (KB) 10^3 byte	1 Kilobyte: half of a typed page 100 Kilobytes: a low-resolution image
Megabyte (MB) 10^6 byte	1 Megabyte: a short book 10 Megabyte: one minute of high-definition audio 100 Megabyte: one shelf of books
Gigabyte (GB) 10^9 byte	1 Gigabyte: a pickup truck filled with books 10 Gigabyte: an inch stack of CDs 100 Gigabyte: a library floor of books
Terabyte (TB) 10^{12} byte	1 Terabytes: 50,000 trees made into paper and printed or 1,500 CDs 10 Terabytes: all of the print collections of the Library of Congress
Petabyte (PB) 10^{15} byte	1 Petabyte: five years of NASA's Earth Observation System data 2 Petabytes: all U.S. academic research libraries 20 Petabytes: amount of data processed by Google per day in 2008 200 Petabytes: all printed material in existence
Exabyte (EB) 10^{18} byte	2 Exabytes: total volume of information generated since 1999 5 Exabytes: all words ever spoken by human beings
Zettabyte (ZB) 10^{21} byte	1.3 Zettabytes: estimated internet traffic in 2016

It is not only information per se that is proliferating, but the variety of channels used to transmit it. Those who wish to monitor and respond to events must select among these channels.

The 2008 financial crisis is an example where information that indicated a problem was widely available, yet difficult to detect. A rare few saw the warning signs, but the vast majority of those affected were taken by surprise. In retrospect, it's fairly clear what happened – so why didn't we see it coming? Simply, the financial system was, and continues to be, far too complex to be parsed and predicted.

Even in areas where the proliferation of information was expected to have obvious positive impacts in the form of transparency results have been mixed. The ubiquity of mobile devices equipped with cameras has led to many major and minor events being captured on video, often from multiple viewpoints. While in some cases video evidence is clear cut, in others it still leaves events open to interpretation. Moreover, video clips can be doctored with increasing realism, or claim to show an event that is actually sourced from a different event. With little or no recourse to verify authenticity, the suppliers of this information must either be taken at their word, else the viewer must accept uncertainty.

We are discovering it's not about having more information, it's about having the right information.

(2) Social Fracturing and Unrest

The Arab Spring (2010-2012) was perhaps the first demonstration of the power of social media to enable large groups to rapidly self-organize and upset established power balances. No central leaders were necessary. Instead, calls to action swept like waves rapidly across populations in viral messages through online social networks. Many long-standing autocracies were toppled, and a chain of events was set into motion that is still being felt today. While popular uprisings are themselves not new, the pace, scale, and contagious nature of the Arab Spring were made possible by the proliferation of information tech.

More generally, deep sociocultural divides in the U.S. and across the world have been exposed in recent years. While many expected the free flow of information across the internet to minimize the perception of our differences, the actual effect has been quite the opposite. Social spaces on the internet have self-segregated into "echo-chambers" where those with similar worldviews aggregate. Interactions between these echo chambers are much less frequent, and often hostile.

The decentralization of media sources has exacerbated these divergences. Niche and alternative media providers deliver information in line with their audience's viewpoints and prejudices. Moreover, mainstream outlets have been forced to 'pick sides' to retain and encourage viewership.

These dynamics of divergence have led to challenges for governance. Uniform decisions and policies that were generally seen as tolerable solutions are no longer tenable. Conflicts in fundamental assumptions about the role of government are making consensus legislation all but impossible. Moreover, every small movement in Washington is visible for the masses to observe via their selected media lens, inducing political paralysis as politicians look towards the next election cycle.

Governance must evolve to work with, and not against, natural forces of self-selection and group formation. Moreover, policymaking must be designed in an iterative fashion, incorporating regular feedback from all stakeholders in order to adapt and ensure that policies work in both current and future environments.

(3) Hybrid Warfare

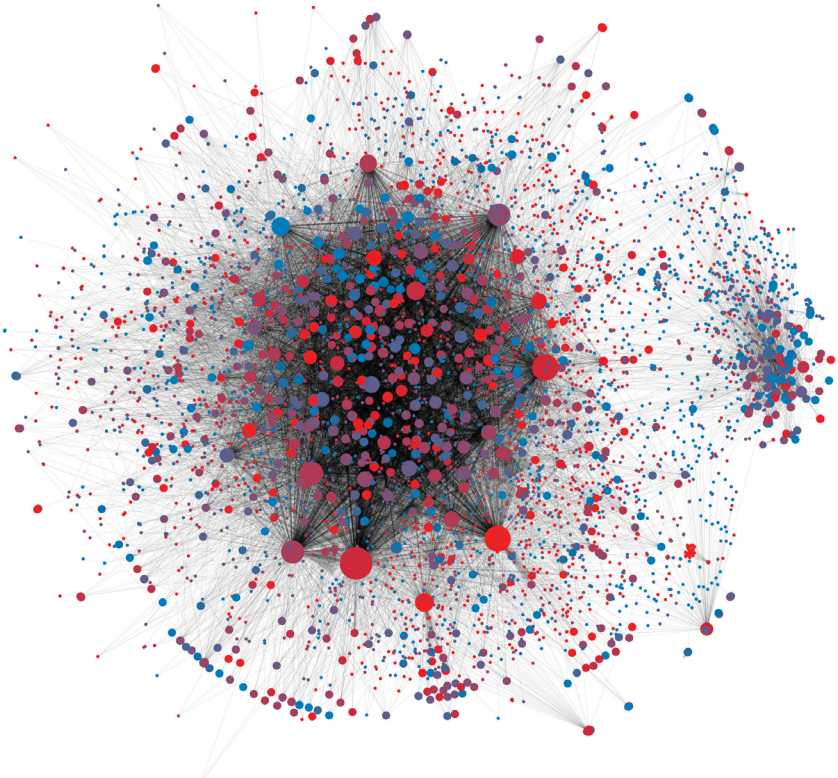
As warfare continues to evolve, information as both weapon and shield has become an increasingly central component. Weaponized information can be designed to have various effects, including influencing populations with selective or false information, creating confusion and disorientation, gaining leverage over key individuals with compromising information, and intercepting and exposing classified information to undercut strategy.

Russian strategy is perhaps the most overt example of information warfare in the 21st century. Their annexation of the Crimean peninsula in 2014 displayed their propensity and willingness to enhance operations with information manipulation. While official Russian sources denied their entering Ukrainian territory, unmarked and masked military forces that became known as "little green men"

played key roles in supporting Russian interests in the conflict. Most commentators agree that these were almost certainly Russian soldiers, but the combination of official denial and a lack of Russian state markings on soldiers and equipment provided doubt and worked in Russia's favor.

THE RISE OF SOCIAL BOTS

ONLINE DEBATE ON CALIFORNIA'S VACCINATION LAW



This network visualization created by Emilio Ferrara in July 2016 illustrates how bots affect online debate about vaccination policy.

Each node represents a Twitter user that tweeted about the #SB277 hashtag (California's vaccination law). Links shows how information spread. The node size represents influence measured in how many times the user was retweeted. Node color indicates likelihood of being a bot or human with red being a bot and blue being a human.

Link to full article

Social media platforms like Twitter and Facebook have opened up new fronts in this battle. The difficulty in verifying the authenticity of users is exploited by those with an agenda. Both human and algorithmic propagandists can pose as organic users simply sharing their opinions. This mimicry of bottom-up activity designed to influence citizens and decision-makers is sometimes referred to as "astroturfing", a play on words that indicates these "grassroots" movements are fraudulent.

State actors are not the only ones leveraging information technologies to their advantage. Virtual social environments have enabled decentralized networks of loosely affiliated parties to act in concert under a common banner in a way that can best be described as 'branding'. The "ISIS" brand has been the most prominent of these in recent years. This hybrid organization, part localized, part non-local, can both attract foreign fighters to their physical strongholds and provide support, both logistical and psychosocial, to malcontents living far away. We lack even appropriate language to address individuals who are willing to commit violent acts in the name of an organization that they may have only ever interacted with online.

New policies and approaches are needed to combat this array of threats that the new environment has given.

(4) Systemic Vulnerabilities

While information warfare is often focused on the manipulation of information to influence human decision-making, a distinct vulnerability has emerged as a result of the rise of the IoT. The reliability and availability of the internet has led to virtually everything being connected, including critical infrastructure such as power grids, communication systems, financial and banking systems, cameras and microphones on computers and smart TVs, and voting machines. These connections enable low-cost transmission as well as remote control, monitoring, and maintenance of systems that would otherwise have to be serviced locally at higher cost.

While there are attractive aspects of making everything available online, the risks have to be weighed carefully. Clever hackers from half a world away can potentially gain access to systems that are literally the foundations for modern life. There is an ongoing arms race in cybersecurity, and nothing that is accessible via the web is entirely secure.

PATHS FOWARD

While there is no one-size-fits-all solution to the myriad challenges posed by the new information environment, some initial pathways towards solutions do exist.

(1) Filtering with Advanced Analytics

In order to sift through the environment to discover information that is relevant to achieving objectives, sophisticated filters must be developed and leveraged. Some of these filters already exist in the form of advanced analytic approaches in the field of complex systems and network sciences. These methodologies include the ability to discover non-obvious points of influence in networked systems, early detection of the potential for extreme events, and discovering large-scale patterns and anomalies.

Machine learning and artificial intelligence approaches can be used to parse large amounts of data. However, these approaches are best suited to tasks where routine decisions can be made without the need to understand how they are made, and where mistakes are tolerable. For many problems, systems that leverage the complementary strengths of artificial and human cognition (i.e. “human in the loop”) will be appropriate.

In all of these approaches, a sensitivity for being misled by the available information must be maintained. Not only do mis- and dis-information pose a challenge for analytic techniques that depend on the data that are supplied to them, but the more sources of data that are leveraged, the greater the number of false relationships that can masquerade as meaningful patterns.

(2) Towards Agile and Adaptive Organizations

The ability to detect relevant information and respond in an agile way is not only a matter of which techniques are applied -- having the right organizational structure is essential. Traditionally, organizations have been structured in hierarchies. Those at the lowest levels interface with external systems, both collecting information and taking action. Those at higher levels receive information from the lower levels, and use it to make decisions and issue instructions. As information ascends the hierarchy, details are lost as a result of convergent information pathways and the inherent limitations of individuals to process information. Instructions issued from central decision makers constrain the actions of those below them, ensuring that they act in concert.

Hierarchies have worked well historically because they make routine processes efficient. Redundancy of effort is minimized, and decisions of those near the top of the hierarchy can be readily amplified leading to large-scale action. However, these same features make hierarchies potentially insensitive to relevant information, and slow to respond to changes in the environment.

When the environment an organization operates in is fast-paced and complex, like that of the new information environment, hierarchies prove to be too rigid to adapt and respond effectively. Instead, flatter, smaller, and less centralized organizations thrive. Smaller, networked organizations are able to respond rapidly to what is locally relevant, rather than having to pass every decision point up the chain of command and wait for instructions to come back down. Moreover, they are able to adapt through rapidly iterating their approaches to problems -- a time-consuming and expensive process for a large hierarchical organization. Approaches to problem-solving that leverage small, self-organizing teams are already proving their value in complex tasks such as software development and special operations.

The new information environment presents new risks, but also novel opportunities. Those who learn to filter through the noise and maintain agility in the face of uncertainty will be the ones who win the day.

Neptune Advisory

202-827-0277
www.neptuneasc.com

415 8th Street SE
Washington, DC 20003

Scott Ellison scott@neptuneasc.com
David Schopler schop@neptuneasc.com
Joe Norman jnorman@neptuneasc.com
Kevin Jiang kevin@neptuneasc.com