INTERNET OF THINGS: VIRTUAL BENEFITS, REAL RISKS

ALEXANDRA KULIKOVA,
GLOBAL STAKEHOLDER ENGAGEMENT MANAGER FOR EASTERN EUROPE AND CENTRAL ASIA AT INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN). CONSULTANT AT PIR CENTER.

The original version of the article in Russian is published in Security Index Journal 2015 Fall №3.

"The headline I fear is, 100,000 fridges attack Bank of America."
Vint Cerf[1]

THE OCTOBER 21, 2015 version of the family home of Marty McFly (he of the "Back to the Future" fame) looked impressively futuristic 30-odd years ago, when the movie came out. Now that the real October 2015 has come and gone, our homes look positively backward compared to the 1980s vision. Nevertheless, some elements of the *smart home* already exist. Virtual reality is making breakneck progress; it is changing our day-to-day lives and our ideas of what that life should be, blurring the line between *online* and *offline*.

INTERNET OF WHAT?

According to Recommendation ITU-T Y.2060 (06/2012) by the International Telecommunications Union, the Internet of Things (IoT)[2] is defined as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)". The concept of IoT was conceived at the Massachusetts Institute of Technology (MIT), where the Auto-ID Center group, founded in 1999, worked on the radio-frequency identification (RFID) and new sensor technologies. Auto-ID Center included experts from seven research institutions on four different continents. It is they who designed the underlying architecture of the future IoT.

A report by *Cisco Internet Business Solutions Group* (IBSG)[3] suggests that the very concept of the IoT emerged when the number of Internet-connected *things*, or devices, surpassed the number of people on the planet. This happened sometime between 2008 and 2009. In 2003, there were 500 million Internet-connected devices in a world of 6.3bn people (0.08 devices per person). By 2010, explosive growth of mobile technology had produced 12.5bn devices in a population of 6.8bn (1.84 devices per person). Of the total population of our planet, only about 2bn are active Internet users, so there were 6.25 Internet-connected devices per active user. In 2010 Cisco specialists predicted that the number of devices would rise to 25 billion by 2015, and 50 billion by 2020.

Gartner[4] offers a somewhat less ambitious projection of 25bn Internet-connected devices by 2020, but does not dispute the sharply upward trend. There is no longer any doubt that the IoT has arrived. It is already altering our ideas of personal and social relations, of business and economics, and of the risks and threats we all have to face. This is a natural result of the rapid rise and spread of ICT, which will attain a whole new level now that the digital divide is closing and the developing countries are also joining the game.

Meanwhile, the evolution of ICT shows no sign of slowing down. In addition to the old and linear user-device relationship, it has produced a new relationship between two or more Internet-connected devices in which the user is the end beneficiary but not an active participant. In other words, the machine-to-machine (M2M) exchange of information in pursuit of some user-defined task is turning the Internet of Things into the Internet of Everything, or the all-encompassing Internet.

In many ways, that process reflects the general post-industrial trend in which the economy of knowledge and the mediatization of social relations with ubiquitous use of ICT reach a whole new level. The new wave of Internet technologies that enable the generation, perception, collection, analysis, and transmission of what is called big data on a massive scale, is changing the information consumption patterns and daily lifestyles of millions of people. It is also shaping their expectations of the future[5]. Back in the 1970s, the Canadian philosopher Marshall MacLuhan described the electronic media (limited to TV and radio in those days) as *an extension of the human nervous system*. One of his key conclusions was that *the medium is the message*; that is, the medium of communication changes man and society in and of itself. That statement is as relevant as ever now that the ICT has penetrated all aspects of our daily lives in the form of billions of various gadgets. Its true essence, however, is probably best applied to the integration of connected devices into a *Network of Networks*, which radically transforms the scale of its impact on human society.

As a result of the growing digitization of the human environment, we now see the emergence of complex local networks of interconnected devices that form a big part of our lives. For example, IDC defines the IoT as a Network of Networks of uniquely identifiable terminals (i.e. things) that interact without human participation through IP connectivity. That ecosystem currently includes devices (including wearables), IoT platforms, servers, security software, industrial process control software, IT services, etc.

The IoT is making inroads in every imaginable sector, such as consumer appliances, the auto industry, healthcare, fashion, transport, road infrastructure, city infrastructure, payment systems, toys, education technologies, weapons, etc. The IoT showcase is wearables such as fitness trackers, as well as augmented reality devices and technologies[6], in which sensors use data about the user's actions and condition to provide relevant visual information or services.

According to *Gartner*[7], about 38 per cent of U.S. consumers have recently used the *virtual assistant* function built into their gadgets. The expectation is that by the end of 2016, two thirds of consumers in the developed world will use virtual assistants on a daily basis. Technologies for automated prediction of the user's requirements based on his or her behavior and location are making rapid progress, and will become increasingly popular as our lives grow ever more hectic.

The Smart Home concept, in which every smart device has its own IP address – including connected electric appliances, cars, hearing aids, and even items of clothing – is a product of scientific discoveries made in the past two decades. This concept is genuinely changing our lives and turning science fiction into reality. In January 2014, Google acquired *Nest*8, a maker of Internet-connected thermostats, for 3.2bn dollars. Nest thermostats are already very popular in the United States and Canada. They not only automate all the processes required to maintain the optimum indoor temperature, but actually study their owner's habits and change the heating or cooling schedules accordingly. Six months after its acquisition by Google, Nest announced the launch of an applied programming interface that enables the makers of various home appliances and other products to make them compatible and interoperable with Nest devices. Unfortunately, it took hackers no time at all to find a vulnerability in the Nest software, and the system can now be hacked in a matter of minutes. Still, hundreds of other companies are also working on smart home technologies, and the smart home market undoubtedly holds a lot of promise.

NEW ECONOMIC HORIZONS

According to an *International Data Corporation* (IDC)[9] study, the global IoT market will grow at an annualized rate of 16.9% in the coming years, from 655.8bn dollars in 2014 to 1.7 trillion in 2020. The company believes that devices, connectivity, and IT services will account for the bulk of that market (about two-thirds) by 2020, while devices (modules/sensors) alone will represent 31.8% of the total. Over the next five years, platforms developed specially for IoT, applications, and AAS solutions will also increase their market share.

A study by *RAND Europe*[10] estimates the economic potential of IoT at somewhere between 1.4 trillion dollars a year to 14.4 trillion across all sectors. Sales of connected devices are projected to reach 2.5 trillion dollars in 2020. In other words, the IoT market is still nascent, and is projected to grow at a breakneck pace.

Gartner believes that the IoT will have a major impact on the development of new business models, and that it will help to make electronic businesses more effective. The company's recent study[11] has found that businesses and IT specialists have particularly great expectations of the IoT in the manufacturing and retail trade sectors. Another promising area is the use of the IoT for process optimization at the utilities and services companies, in the industrial sector, auto-making, and consumer goods. A case in point is the energy sector, which increasingly relies on sensors and automatic process control systems built into meters, monitoring devices, energy use management systems, etc.

The new opportunities offered by the IoT can transform the existing industrial processes, companies' relations with their consumers, and in the end, our entire day-to-day lives. For now, there are no comprehensive, all-encompassing IoT solutions; we only have individual examples of IoT-driven transformations in individual sectors (health monitoring, wearables, driverless cars, etc.) There is still a lot of mistrust and lack of understanding in the private sector of how exactly each individual business can benefit from the IoT and recoup the cost of implementing these new technologies. Fundamental systemic transformations will probably have to wait for the arrival of a "killer application" or technology that can transform the market on a global scale. It will serve as the first link between the local networks formed by connected devices to perform some specific task or a set of related tasks.

It is safe to say that in five to seven years' time, the IoT will have reached every single sector of the economy and every market. The low cost of sensor technologies might well make other business solutions uncompetitive. The speed of their development and penetration will kill off all the market players who cannot keep up with the trend and are therefore unable to provide the standards of quality and service customers will have come to expect.

Whole businesses built on data are no longer a theoretical proposition; exponential growth of data about users generated by connected devices will make that data the new gold, the new oil, and the new currency of the 21st century – and these are not just punchy metaphors. Information about users has already become an important driver of growth for private businesses. An increase in the amount of that data and a clearer realization of its value by the users will create a new paradigm of managing that information and of the wider social relations. Effective collection, processing, and analysis of the Big Data will be key to the success of many businesses.

The IoT promises to make various business processes more effective – but it may also give rise to new *grey areas.* The replacement of human decision-makers with machines is still at the very early stage, but it is already raising many ethical and economic questions. It is also presenting new challenges in terms of user and data security. For example, a printer that monitors the level of ink in the cartridge and orders a new cartridge online can make its user's life much simpler. But it also means that the printer must have access to all the required information to have the cartridge bought, delivered and perhaps even installed – such as the geolocation data, bank details, information about the specific type of the device for which the cartridge is being ordered and, indirectly, about how often the user prints pages. Automating all these processes will require all the related data to be gathered, processed, transferred, and probably stored as well – with all the associated risks.

HURDLES ON THE WAY TO UBIQUITOUS IOT

The speed and success of the deployment of IoT technologies, and the integration of these technologies into the modern social and economic architecture will depend on a number of factors. First, it will require a complete transition to the new IPv6 protocol from the old IPv4, which has all but run out of the available IP address blocks[12]. Technically, this transition is complicated by compatibility problems, and the speed of the transition will determine how many unique connected devices will come online in the coming years. For example, the American Registry for Internet Numbers (ARIN) ran out of primary IPv4 address blocks on September 24, 2015, although blocks are still available for sale on the secondary market. Some parts of the world are switching to IPv6 much faster than others. This will undoubtedly affect the speed of IoT penetration and the uniformity of the IoT standards being drawn up.

Another important requirement for a rapid adoption of IoT technologies is standard protocols that enable devices to talk to each other and to the user. Common standard will be especially important in such areas as data management security, data integrity and privacy, and integrity of the entire IoT architecture. If these requirements are met, IoT technologies will attain a whole new level, ushering in a new paradigm of the development of human society. As already mentioned, IoT technologies are spreading into almost every single sphere all at the same time; as a result, there is still no universal standard of communication between the various connected devices and solutions. A number of organizations (IEEE, IETF, ITU, ISO, and others) are already trying to tackle that problem, focusing among other things on developing proper mechanisms for uninterrupted transmission of IPv6 packets in networks of various configurations, the complexity of which is only going to increase over time. For now, however, they have yet to develop a universal set of specifications that could be applied to all the areas where the IoT is or will be used.

In May 2015, the ITU-T Focus Group on Smart Sustainable Cities (FG-SSC)[13] completed its work by releasing 21 reports on IoT specifications. Its mandate has been taken over by the ITU-T SG20 (Study Group 20)[14], which will continue efforts to develop a universal set of requirements for IoT standards, with a primary focus on *smart cities and communities* (SC&C). That, however, is just one of the fragments of the rapidly growing IoT market. It is also worth noting that the lack of universal standards for interoperability between devices in the entire IoT ecosystem is also slowing efforts to develop mechanisms of protecting these devices from malicious external impact.

Nevertheless, there are individual examples of standards being adopted in some specific areas, such as sensor-mediated authentication. The growing number of online services and connected personal devices makes password-based security systems increasingly cumbersome and outdated. Biometric authentication (based on fingerprints, retina scanning, or voice recognition) is regarded as an extremely reliable method of user authentication. In the spring of 2015, Halifax, a British bank, proposed a new authentication technology for its online banking system that is based on the user's electrocardiogram[15], which has a unique signature for every individual and cannot be forged.

Meanwhile, the FIDO (Fast Identity Online)[16] industry alliance, which was launched in 2012 and now brings together more than 100 major companies (including MasterCard, Visa, Google, PayPal, and Bank of America) as well as the German federal agency for information security (a member since October 2015), is developing specifications that aim to make online communications more secure using biometric technologies and multi-factor authentication (MFA). For example, Apple has been using fingerprint authentication in its smartphones for several years now; fingerprints can also be used for the Apple Pay service. Microsoft joined FIDO in February 2015, when it announced its intention to use FIDO technologies in its new Windows 10 operating system. So essentially, we have a private-sector alliance developing a universal user authentication standard for electronic devices (Universal Authentication Framework (UAF) и Universal Second Factor (U2F)). Given the size of the companies behind the alliance, there is a good chance of FIDO standards gaining widespread adoption, and perhaps even securing a monopoly in the user authentication technology market.

Finally, providing an uninterrupted energy supply for the huge numbers of various electronic devices is a global challenge. It will require new power generation solutions, powerful servers and energy grids, and technologies of protecting them.

So far, the new technological paradigm is still in the early stages of development and scaling up. The turning point was probably the launch of the first iPhone, which revolutionized the smartphone market. It was a perfect example of destructive innovation (a term proposed by Clayton Christensen)[17] that has taken an entire industry to a whole new level while also delivering a devastating blow to some of the successful long-established businesses. The new priority of user-friendliness proved a winning formula at that stage in IT progress. Meanwhile, the growing ubiquity of the Internet has enabled a rapid expansion of the ecosystem of connected devices. The next leap of destructive innovation will probably center on universal standards, enabling all the connected devices that make the Internet of Things to speak the same language, thereby achieving new synergies. This is what the world is gradually moving towards, and this new scale of the IoT promises both a new quality of life and a whole host of new security threats.

What are the risks?

The unbelievable new opportunities opened up by the ecosystem of connected devices acting as part of a single network go hand in hand with new risks. Those risks can seriously undermine social and economic progress. What exactly are the risks, and how real are they?

Cybersecurity of Everything?

As the number of Internet-connected things grows, so does the number of potentially hackable devices. This a natural and inevitable downside of the development of digital society; security measures often struggle to keep up with technological innovation. So, to borrow a phrase coined by Kaspersky Lab, IoT can stand not only for the Internet of Things, but also for the Internet of Threats. The scale of those threats is directly proportionate to the scale of digital progress. According to the insurance giant Lloyds, cyberattacks cost companies around the world 400 billion dollars a year. That figure includes the damage itself and the cost of disruption caused by these attacks. Interestingly, about 90% of cyber insurance is being purchased by U.S. firms[18].

The growing number of connected devices makes it increasingly more difficult to attribute cyberattacks because there is a growing number of hubs through which these attacks (such as anonymized DDoS attacks) can be routed. In other words, it is becoming ever more likely that one of your devices may at some point become an accomplice in a cyberattack, completely unbeknownst to you.

In July 2015, the *Wired* magazine reported[19] that two hackers had demonstrated the possibility of using a software vulnerability called *Zero-day exploit* to take remote control of a Jeep Cherokee after hacking its Internet-connected multimedia system. As the journalist who did the experiment traveled in the hacked car at 70 miles per hour, he watched the hackers remotely change settings on his climate control and radio, turn on windshield wipers, and then cut the transmission. All he could do was hope for the best, unable to control his own vehicle.

That was the first such demonstration. In addition to being great PR for the hackers involved, and an important lesson for Chrysler, it threw into stark relief the *other side* of digital technologies penetrating all spheres of our daily lives – especially in situations where keeping a connected device from running amok can be a matter of life and death. The digital interface of many systems and devices makes them that much easier for the user to operate, but it also makes them vulnerable to cyber-intrusions. The dangers include unauthorized access to user data, corruption of that data, personal data theft, financial theft, acts of sabotage against industrial infrastructure, etc. Finally, enormous opportunities are opening up for cyber-espionage. The amount, topology, and granularity of the data available online hold a great promise of convenience for the end user, but they also raise the prospect of major damage caused by that data falling into the wrong hands.

The deeper IoT technologies penetrate our social and economic systems, bringing together a growing number of key network elements, the more serious the potential consequences of a hacker attack. Hackers breaking into IoT devices that make up an interconnected digital society infrastructure can cause the same kind of trouble as old-school hacking on individual standalone devices – but on a much grander scale. For example, a city running a *smart energy grid* can make huge savings by optimizing energy flows, but it also becomes a vulnerable target for hackers, and a single hacking incident can have catastrophic consequences for the entire grid.

A case in point is the massive blackout in the northeastern United States and Canada[20] in 2003, which left 40 million Americans and 10 million Canadians without electricity, and forced closures of several international airports in both countries. It turned out that the blackout was caused by an error in the software operated by the energy utility FirstEnergy in the state of Ohio. As a result of that error, grid controllers did not react in a timely manner to a short circuit caused by overheated street wires sagging and touching a tree. Had that single short circuit been quickly isolated, the problem would not have cascaded to affect tens of millions of people. It is easy to imagine similar scenarios caused by a malicious act rather than an error – targeting, for example, the monitoring systems of other elements of a smart grid. Incidentally, dangers such as this one are precisely the reason why the control systems at some critical infrastructure facilities (such as nuclear power plants) are deliberately being left stuck in the analogue age instead of upgrading them to new IT technology.

The interdependence of various systems can cause a domino effect, leading to grave consequences, including human casualties. In April 2015, the U.S. Government Accountability Office released a report[21] warning that modern airplanes' connection to the Internet and their growing cyber-reliance on ground systems "can potentially provide unauthorized remote access to aircraft avionics systems". These new interconnected systems installed on the latest planes now require a separate certification process with the Federal Aviation Administration; there are also plans for a complete review of cybersecurity requirements for all avionics systems.

Meanwhile, auto makers are also trying to produce universal standards[22] using the *safety by design* principle, meaning that measures to minimize cyber risks are taken early on during product R&D.

It is safe to say that any projections for the growth of the IoT market must take into account the inevitable cybersecurity incidents that will cost billions. Such incidents are bound to happen because connected products' defenses against cyber-intrusion are often developed after these products hit the shelves. Since the IoT market is still far from maturity, players are trying to seize a share of that market as early as possible. As a result, they tend to shunt aside any concerns that could potentially delay product launch – including cybersecurity concerns. In the future, once the problem of protecting users and their data in the IoT context becomes even more obvious, the market for IoT cybersecurity products will become another major growth driver, spurring fierce competition among the developers of such products.

THE ETHICAL SIDE OF THE COIN: PRIVACY

As we discuss the future of the IoT on the global and local scale – especially in the context of security – let us not forget that the IoT is also increasingly transforming the approaches to online privacy. Debates about the right to privacy (enshrined in such international documents as Article 12 of the UN Universal Declaration of Human Rights[23], Article 8 of the European Convention on Human Rights[24], and Article 17 of the International Covenant on Civil and Political Rights[25]) have become especially relevant after the revelation in the summer of 2013 of mass electronic surveillance by the U.S. National Security Agency (NSA). New opportunities for mass snooping are also being opened by the technology companies that build their business on targeted advertising that is based on information about individual users' activities and preferences. In addition to the personal and communication data that have long been available, companies are now also gaining access to geolocation, biometric, and other information that enables them to build an increasingly accurate portrait of each individual user and his or her daily activities. This opens breathtaking vistas for advertisers and other actors who want to know as much as possible about every specific individual or groups of people, for legitimate or nefarious purposes.

The rise of the IoT takes the privacy problem to a radically new level; attitudes to that problem and approaches to resolving it will vary depending on how well each individual community tolerates mass data gathering. We can assume that the development of IoT technologies will be more rapid in the United States, for reasons of America's historically more liberal attitude to personal data gathering and its lack of a single regulatory instrument in this sphere. Witness, for example, the latest instalment in the old saga of America and the EU trying to harmonize their trade relations and resolve the related issue of personal data transfers across the national borders[26]. Furthermore, the boundary between the public and the private in cyberspace is becoming increasingly blurred as the amount of user data generated, processed, and transmitted online continues to grow; the existing instruments do not fully take this particular circumstance into account.

Nevertheless, even those societies that don't have much of a problem with public availability of online user data will inevitably realize that the user agreement is not entirely fair. How adequate is the price users pay for *free* services such as web search, email boxes, or IoT technologies by surrendering their personal data, which are then used for commercial purposes?

As already mentioned, the scale of this symbiosis will continue to grow, as will the risks related to the leakage or corruption of user data. Meanwhile, the business model itself will continue to develop as more IoT-connected devices become platforms for user data generation. For now, we are talking about anonymized and aggregated data – but personal attribution of such data can easily be restored by comparing various data categories. Besides, as IoT technologies become an ever more ubiquitous part of the basic infrastructure of our daily lives (utilities, healthcare, transport, etc.) it will become increasingly difficult to forego their use. The user still has the right to adjust their privacy settings to their individual liking – but at the cost of losing some of the services. Another alternative is just to decline the user agreement completely.

One of the best examples of this trend is the growing popularity of virtual assistants[27]. Apple launched its Siri assistant back in 2010, complete with such functionality as searching for information, sending text messages, making phone calls, scheduling appointments, and placing online shopping orders by giving voice commands. Siri has since been followed by Google Now, Microsoft's Cortana, Facebook M, and even Duer, developed by China's Baidu. Over time, the convergence of various mobile services will expand the functionality of virtual assistants, and data searches will be performed taking into account everything the virtual assistant already "knows" about its owner.

According to Gartner, 38% of U.S. gadget owners have recently used the virtual assistant function built into these gadgets. The current projection is that by late 2016, about two thirds of users in the developed markets will do so on a daily basis. As big data analysis, voice recognition, and artificial intelligence technologies continue to improve, so will the usefulness of virtual assistants. Also, as the amount of the information being processed increases, users will be ever more inclined to offload part of their work on a capable electronic assistant. It is, however, important to remember that virtual assistants' independence in decision making, combined with access to user data granted to various applications installed on the user's smartphone, creates a potentially problematic situation with centralizing control over all that data. Centralization always increases a system's vulnerability. For example, a debate is now under way[28] about the Windows 10 operating system's aggressive policies on collecting user data, including data collection by Cortana. According to some reports about the Cortana algorithms, that virtual assistant sends some user data to Microsoft servers even if the user has opted out of using Cortana.

Some of the smart TVs made by Samsung also have built-in voice recognition. The microphone can of course be switched off – but the possibility of it being switched back on again remotely, unbeknownst to the TV's owner, undermines the owner's confidence that they control privacy in their own home.

In this context, the user would be entirely within their right to demand a revision of the whole deal, and a new, more transparent report by communications companies on making user data available to third parties, i.e. their commercial partners, which are usually referred to in user agreements as "trusted third parties". This also has implications for fair competition and equal access to the services of various third parties. Of course, virtual assistants will have an option to default to a specific trusted third party for various user-requested services, unless the user specifies which particular party he wants. For example, if a user asks his or her virtual assistant to call a taxi, it can default to Uber rather than, say, Gett. The user will still be able to make the final decision and choose his or her preferred service provider. Nevertheless, as our lives become more hectic, there will be a growing scope for virtual assistants to make these day-to-day decisions completely on their own.

It is important to understand that we are not just talking about the philosophical issue of finding the right balance between privacy and convenience. This is also about how comfortable users will be with disclosing information about themselves to the outside world without being in full control of where that information ends up, who has access to it, and how it can be used today, tomorrow, or the day after. Unauthorized or uncontrolled access to an individual's medical data gathered by wearables, sensors built into closing, fitness gadgets, etc. – let alone the data and conversations stored on PCs or smartphones – can be misused and abused by insurance companies, employers, business partners, etc. Last year, there was a discussion in the UK about legalizing the sale of patient databases maintained by the NHS (the National Health Service) to pharmaceutical and insurance companies[29] - including such data as ID numbers, birth dates, gender, ethnicity, and postcode – *in order to improve the quality of service*. The measure has not been implemented, but breaches of such data are already a regular occurrence. Meanwhile, the growing number of various user applications that make use of those data increase their vulnerability even further. Intrusions and theft by hackers are also all but inevitable[30].

In a situation where user data is increasingly being seen as the *oil of the 21 century*, or as *new currency*, it becomes blindingly obvious that if you are a being offered a free product, you can be certain that the real product is you. That is why the growing number of *smart device* makers that join the IoT ecosystem will have to build a relationship of trust with their users, with total transparency and detailed reporting about how user data are being used by the company itself and by its partners. Responsibility and diligence in this area will become part of the corporate brand, and data security measures a new way of gaining competitive advantage over rivals. It is quite possible that at some point in the future, industries will develop new best practices by means of self-regulation, in addition to rules introduced in national legislation and regional bylaws.

For example, a growing number of technology companies regularly publish transparency reports[31]. The practice was initiated by Google in 2010: after it withdrew from the Chinese market, it began to publish statistics on national governments' requests for disclosure of user data or for the blocking of various content. In 2013, Edward Snowden's revelations about the use of IT companies by the secret services for electronic snooping gave a fresh impetus to the practice of transparency reporting; by that time, such reports were being published on a regular basis by at least 10 major IT companies. In an effort to reassure their users, a growing number of companies are now following the example set by Google. In the future, law-enforcement and security agencies will undoubtedly send their user data requests to more companies; there will also be more of the various data to request. As for the transparency reports, they should also include information about the nature of the relationship with *trusted third parties* – that is, commercial partners. At this time, transparency reports do not normally specify the precise information that has been requested by governments. But as the amount and the granularity of the data increases, companies will inevitably have to think about improving the procedures of reporting both to the governments and to their own users.

Another promising area is the use of open data, platforms, and standards, which would make less relevant the problem of finding the right balance between profit and privacy.

WHO IS TO BLAME?

Another important question without an obvious answer is who (or what) is responsible for any incidents involving smart devices, and for the resulting damage. If a device has elements of artificial intelligence and makes independent decisions, should it also be held responsible for the consequences? Operator-independent M2M communications, in which decision-making is delegated to machines, blur the boundary between the *actor* and its *instrument*[32]. Who or what exactly is the actor, and who has agency: the human operator that delegates decisions on replacing a spare part to the machine, or the machine itself, which supplies the human operator's bank details to an unreliable online shop that sells the spare part? Insurance companies will have a particular interest in finding the right answer to that question.

Furthermore, the aforementioned problem of user data being generated and transferred by smart devices to third parties will become especially pressing as devices become increasingly interconnected, with instantaneous data processing and exchange. Which particular device (or devices) has "ownership" of the data, and which device is responsible for the security and integrity of that data?

RULES OF THE GAME

There are now many more questions than answers because the body of regulations for managing and minimizing all the existing risks has yet to be put in place. Some countries, such as the United States and South Korea, deliberately pursue a policy of regulatory nonintervention while the companies are fighting to secure a share of the IoT market, and while the direction of the IoT industry's technological and economic development remains unclear. This is recognized in a June 2015 ITU report[33] in IoT regulation. There are many uncoordinated studies and regional attempts at channeling the development of the IoT, or at least getting a clearer idea of the potential challenges. The problem is that, as in the rest of the IT industry, regulatory efforts often fall well behind the already available technology and products. Also, the steps being taken are sometimes mutually contradictory. For example, at a conference held in March 2015 in Brussels by the European Commission, technological companies discussed the need for lifting the obstacles to the development of the IoT in Europe, especially in view of the fierce competition from U.S. and Chinese rivals. Europe's high Internet penetration rates and the EU's Digital Single Market program can stimulate the development of IoT technologies. But at the same time, Europe has such clear obstacles as the already mentioned differences over the protection of personal data when it crosses the national borders.

The United States is investing huge resources into the IoT – but these efforts are being held back by the poor penetration rates, low speeds, and high cost of broadband Internet access in the country. The Federal Trade Commission has recommended that the government desist from any direct IoT regulation – probably in the hope of facilitating rapid technological progress without any restrictions. Nevertheless, various government agencies are well aware of the existing and potential risks. For example, the FBI has issued guidelines on managing new cybercrime risks arising from the spread of IoT technologies[34]. As already mentioned, the lack of universal and global IoT standards is holding back the entire industry. Still, the private sector is pinning great hopes on the IoT. For example, in the spring of 2015, IBM announced an investment of 3bn dollars into its new IoT division. Awareness of the standardization problem is also encouraging private companies to seek cooperation and coordination in order to optimize their business processes.

In 2014, the Internet and technology giants IBM, Cisco, General Electric, Intel, and AT&T formed the Industrial Internet Consortium[35] to facilitate the development of engineering standards for industrial IoT devices, share best practice, test new products, and coordinate research in the area of safety and security of new technologies. The consortium has since been joined by numerous large and small companies, research centers and universities, and government organizations. The IIC includes a separate Security Working Group[36].

China is one of the leading players in the IoT field. In fact, it invests more into this sector than either Europe or the United States. According to RAND Europe, in 2012 the Chinese spent 625m dollars on developing IoT technologies. The Chinese Ministry of Information and Technologies has also set up a 775m-dollar fund to create techno parks all over the county over a five-year period. In 2013, the Chinese government established an inter-agency council for coordinating government policy and initiatives on the IoT[37]. In 2013 the council contributed to a new government directive and working plan for IoT development, with specific goals for the development, standardization, application, and rollout of products, business modeling, regulation, and training.

For the time being, however, the size of the Chinese market is way ahead of its consumer maturity. There is also a huge potential in the entire Asia Pacific Region, where the most mature markets in terms of the per capita numbers of connected devices are Australia, New Zealand, and South Korea. According to the research company IDC[38], the IoT market in the AsPac region (excluding Japan) will grow from 250bn dollars in 2013 to 583bn in 2020. The number of connected devices in the entire region is projected to rise from 2.59bn in 2013 to 8.98bn in 2020. Nevertheless, this market is still in the early stages of its development, and the makers of smart devices are not focusing on the existing and future security threats because such a focus would inevitably increase their development, manufacturing, and distribution costs. Still, many large companies with a strong presence in the region[39] – such as Cisco Systems, Fortinet, and Check Point – are already well aware that the issue must be addressed without delay, so that the development of their future products could take into account certification requirements and other regulatory compliance issues. So far, there is no clear set of rules or procedures in this area.

In Russia, the consumer IoT market is being formed predominantly by foreign gadget makers, but in view of the recent import substitution trend, there is now more emphasis on domestic R&D. The broadband penetration rates in Russia are fairly high, so the outlook for the IoT market is positive. Unsurprisingly, Rostelecom[40], the country's largest telecommunications operator, is one of Russia's IoT pioneers. It plans to make a major contribution to structuring the national market for the industrial IoT. To that end, it wants to borrow the experience of the aforementioned Industrial Internet Consortium, which it has joined in order to gain access to case studies, research, and emerging standards. There are now plans for setting up a Russian equivalent of the IIC, called Association for Facilitating the Development of the Industrial Internet in Russia. The body should be up and running by the end of 2016. Growth opportunities in the various Russian industries and the potential for their integration on the huge Russian market promise great economies of scale. Rostelecom expects that industrial companies will be the first to join the new Association, followed by the suppliers of technological solutions and expert groups. For example, a preliminary agreement has already been reached with the Russian Space Systems (RKS) on the use of industrial Internet technologies in the space industry.

These efforts undertaken by a single Russian company are clearly inadequate in view of the size of the Russian market; nevertheless, they are timely and very important. The Internet of Things, including the Industrial Internet, is one of those areas of global development where the rules of the game are being written and the roles are being distributed right at this moment. Russia has a great opportunity not to miss out on this latest spurt of technological progress, and to become an important player at least in some of the most promising markets, both local and perhaps even global, before foreign companies irreversibly seize the initiative. These markets include the defense industry, the financial sector, transport, etc. The ongoing crisis in the global economy and the local Russian trend towards import substitution create a favorable climate for achieving such a goal. For now, Russia does not have an extensive toolkit of regulatory instruments for the IoT industry – but its government is making a strong emphasis on protecting personal data of Russian citizens (a case in point is Law 242-FZ, under which all personal data of Russian citizens must be stored on servers in Russian territory from September 1, 2015). That emphasis will make a strong contribution to the development of the IoT ecosystem, especially in terms of security.

The security aspects of the development of the industrial IoT will inevitably be discussed in the context of international cooperation on responsible conduct in cyberspace. The voluntary code of conduct agreed by the UN Group of Governmental Experts in the summer of 2015 includes not attacking critical infrastructure facilities and not implanting malicious software functionality into IT products. There is also a whole range of confidence-building measures such as exchange of information about the existing vulnerabilities and risks, providing assistance to CERT/CSIRT rapid response groups, etc. If these agreed measures were to be fully implemented, the development of the industrial IoT in countries around the world could be underpinned by reliable cybersecurity arrangements agreed at the highest level. But despite that trend towards internationally agreed rules of the game in terms of nation-states' conduct in cyberspace, the degree of mutual confidence on the global arena is still insufficient for these rules to be always observed.

On the lower level of user devices, one of the major risks is the ongoing debate about the need to weaken end-to-end data encryption in communication products in order to facilitate the work of law-enforcement and security agencies' investigators. Such a possibility is already being discussed in the United States and the United Kingdom. If these two countries implement such proposals, other governments will follow suit. Experts believe, however, that effective data encryption can either be secure for all – including criminal actors – or insecure for all. The public debate is still ongoing, and its outcome will largely determine the level of user confidence in new IoT products. Still, in countries where the public has a fairly high level of confidence in their government as the guarantor of national, public, and individual security, this problem may never fully arise.

CONCLUSION

The Internet of Things is at a very interesting phase in its development. Its social and economic potential to change people's lives in many different areas has already been realized (though perhaps not fully). Countries and companies around the world have also become aware of the need to seize a dominant position in the process of IoT development and thus secure a head start for themselves before the competition begins in earnest. Finally, the regulatory framework is only just taking shape and remains quite flexible, leaving a lot of room for innovation and competitive struggle.

It is also clear that the security risks that have already come to the fore are holding back the development of the IoT market; on the other hand, they also open up a competitive niche. The leaders of that market realize the need to take security into account at the very early stages of R&D, even universal standards of device interaction or device/user security become available.

We can expect continued efforts at establishing common sets of rules and procedures for the IoT both by the industry itself and by government regulators – though the latter will probably tend to lag behind industry development. Success in finding the right balance between being the first to market and ensuring proper security measures will mostly depend on the expected social and economic benefit of IoT technologies in each individual society and market, and on the public's expectations in terms of security provisions. It will also depend on the willingness and readiness of specialists in different industries, business leaders, and IT developers on the one hand, and cybersecurity / information security specialists on the other, to arrive at joint technological solutions. Any regulatory decisions must facilitate that dialogue. The result of it will determine whether the IoT will come to be the Internet of Things, or the Internet of Threats.

REFERENCES

[1] Vice President of Goggle and one of the Internet pioneers.

[2] ITU-T Recommendation Y.2060 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (Last accessed October 11, 2015)

[3] Cisco Systems report "How the Next Evolution of the Internet Is Changing Everything" http://postscapes.com/cisco-internet-of-things-white-paper-how-the-next-evolution-of-the-internet-is-changing-everything%20 (Last accessed October 11, 2015)

[4] The Internet of Things Is a Revolution Waiting to Happen, interview with Jim Tully, Vice President of Gartner http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waiting-to-happen/?cm_mmc=social-_-rm-_-gart-_-swg (Last accessed October 11, 2015)

[5] Lecture by Marshall MacLuhan, "Medium in the message", June 27, 1977, given in Australia. http://www.youtube.com/watch?v=ImaH51F4HBw (Last accessed October 11, 2015)

[6] Augmented reality: a space between reality and virtual space

[7] The software secretaries, The Economist, September 12, 2015 http://www.economist.com/news/business-and-finance/21664071-technology-firms-are-competing-become-consumers-personal-secretaries-big-implications (Last accessed October 11, 2015)

[8] Google Nest, https://nest.com (Last accessed October 11, 2015)

[9] Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, IDC http://www.idc.com/getdoc.jsp?containerId=prUS25658015 (Last accessed October 11, 2015)

[10] Europe's Policy Options for a Dynamic and Trustworthy Development of the Internet of things, RAND Corporation http://www.rand.org/pubs/research_reports/RR356.html (Last accessed October 11, 2015)

[11] The Internet of things is a Revolution Waiting to Happen, Gartner http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waiting-to-happen/?cm_mmc=social-_-rm-_-gart-_-swg (Last accessed October 11, 2015)

[12] North America is out of IPv4 addresses—for really real this time, Ars Technica http://arstechnica.com/business/2015/09/north-america-is-out-of-ipv4-addresses-for-really-real-this-time (Last accessed October 11, 2015)

[13] Internet of Things Global Standards Initiative http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (Last accessed October 11, 2015)

[14] (SC&C) ITU-T Study Group 20 http://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx (Last accessed October 11, 2015)

[15] Halifax trials heartbeat ID technology for online banking, Guardian, March 13, 2015 http://www.theguardian.com/technology/2015/mar/13/halifax-trials-heartbeat-id-technology-for-online-banking (Last accessed October 11, 2015)

[16] FIDO Alliance, https://fidoalliance.org (Last accessed October 11, 2015)

[17] Clayton Christensen, professor at Harvard, http://www.claytonchristensen.com/key-concepts (Last accessed October 11, 2015)

[18] Stephen Gandel. Lloyd's CEO: Cyber attacks cost companies $400 billion every year, Fortune, January 23, 2015 http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds (Last accessed October 11, 2015)

[19] Andy Greenberg. Hackers Remotely Kill a Jeep on the Highway - With Me In It, Wired, July 21, 2015 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway (Last accessed October 11, 2015)

[20] Blackout hits New York City and the Northeast in 2003, New York Daily News, August 13, 2015 http://www.nydailynews.com/news/national/blackout-hits-northeast-united-states-2003-article-1.2322074 (Last ac-

cessed October 11, 2015)

[21] FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen, Report by the U.S. Government Accountability Office. April 14, 2015 http://www.gao.gov/products/GAO-15-370 (Last accessed October 11, 2015)

[22] Five Star Automotive Cyber Safety Program, Cavalry https://www.iamthecavalry.org/domains/automotive/5star (Last accessed October 11, 2015)

[23] UN Universal Declaration of Human Rights http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (Last accessed October 11, 2015)

[24] European Convention on Human Rights http://www.echr.coe.int/Documents/Convention_RUS.pdf (Last accessed October 11, 2015)

[25] International Covenant on Civil and Political Rights http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (Last accessed October 11, 2015)

[26] Article 25 (1) of Directive 95/46/EC stipulates that the Member States shall provide that the transfer to a third country of personal data is allowed only if the third country in question ensures an adequate level of protection. In terms of the European legislation, the United States is not considered to be a country where adequate level of protection is ensured. For the purposes of harmonization, the EU has created a mechanism of approval by international corporations of special universal corporate rules for data processing (Binding Corporate Rules, Article 26 (2) of Directive 95/46/EC), and agreed special principles that enable data transfer for individual companies (more than 4,000 of them) (Safe Harbor – EU Commission Decision No 2000/520/E of July 26, 2000). Edward Snowden's disclosures have shown that this mechanism does not ensure adequate data protection. Work is currently under way on new EU personal data protection regulations, which should include a general principle whereby the provisions on the transfer of data to third countries or international organizations should also be applied to any subsequent transfers of personal data from such third parties to other entities (Article 40 of the draft regulation). There are also plans for the abolition or revision of the Safe Harbor mechanism. On October 6, 2015, the European Court ruled that Safe Harbor is illegal and should not prevent EU member states from protecting their citizens' right to privacy, and that EU members should have the power to block the transfer of their citizens' personal data to third countries where necessary.

[27] The software secretaries, The Economist, September 12, 2015 http://www.economist.com/news/business-and-finance/21664071-technology-firms-are-competing-become-consumers-personal-secretaries-big-implications (Last accessed October 11, 2015)

[28] Alexandra Kulikova. Windows 10: Farewell to Privacy, Forbes (Russian edition), August 26, 2015 http://www.forbes.ru/mneniya-column/idei/297823-windows-10-proshchanie-s-privatnostyu (Last accessed October 11, 2015)

[29] Randeep Ramesh. NHS patient data to be made available for sale to drug and insurance firms, The Guardian, January 19, 2014 http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy (Last accessed October 11, 2015)

[30] Kris Simmons. NHS-accredited health apps vulnerable to hacking, CelebCafe, September 25, 2015 http://celebcafe.org/nhs-accredited-health-apps-vulnerable-to-hacking-2120 (Last accessed October 11, 2015)

[31] Alexandra Kulikova. Transparency reporting and confidentiality policies of ICT corporations before and after Snowden, Puls Kibermira electronic journal by PIR Center, No 1 (108), 2014

[32] Agency in the Internet of Things, European Commission report, 2013 https://ec.europa.eu/jrc/sites/default/files/lbna26459enn.pdf (Last accessed October 11, 2015)

[33] Regulation and the Internet of Things, GSR discussion paper https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf (Last accessed 11.10.2015)

[34] Internet of things poses opportunities for cybercrime, Federal Bureau of Investigations, September 10, 2015 https://www.ic3.gov/media/2015/150910.aspx (Last accessed October 11, 2015)

[35] Industrial Internet Consortium, http://www.industrialinternetconsortium.org (Last accessed October 11, 2015)

[36] Security Working Group, Industrial Internet Consortium, http://www.industrialinternetconsortium.org/wc-security.htm (Last accessed October 11, 2015)

[37] How China is Scaling the Internet of Things, GSMA report, July 2015 http://www.gsma.com/newsroom/wp-content/uploads/16531-china-iot-report-lr.pdf (Last accessed October 11, 2015)

[38] Asia/Pacific Becomes the Frontline for IoT, with Industry to Connect 8.6 Billion Things and Create an USD583 Billion Market Opportunity by 2020, IDC, press release of April 9, 2015 http://www.idc.com/getdoc.jsp?containerId=prHK25553415 (Last accessed October 11, 2015)

[39] Eileen Yu. Certification, regulation needed to secure IoT devices, ZD-Net, May 21, 2015 http://www.zdnet.com/article/certification-regulations-needed-to-secure-iot-devices (Last accessed October 11, 2015)

[40] Marina Chernetsova. "In another year's time, it will be too late to build the Russian Industrial Internet", interview with B. Glazkov, Rostelecom, TheRuNet, October 9, 2015 http://www.therunet.com/interviews/4945-cherez-god-stroit-rossiyskiy-promyshlennyy-internet-budet-uzhe-pozdno (Last accessed October 11, 2015)