ORIGINAL ARTICLE

Scenarios for crime and terrorist attacks using the internet of things

Roey Tzezana [1]

Received: 18 November 2016 / Accepted: 24 November 2016 / Published online: 1 December 2016

Abstract The Internet of Things is a paradigm in which everyday items are connected to the internet and share information with other devices. This new paradigm is rapidly becoming a reality in the developed world, and while it holds an immensely positive potential, it also means that criminals and terrorists would be able to influence the physical world from the comfort of their homes. We can expect that hackers, ransomwares, viruses, spywares and many of the other woes of the internet today will migrate to the internet of things as well. In this research we used General Morphological Analysis and brought together fifty experts on an online platform to develop novel scenarios about the crimes and terrorist acts of the future. The experts developed 21 scenarios, which were then ranked according to their plausibility. We provide a brief description of every scenario, and focus particularly on the four most plausible ones: blackmailing by connecting to smart homes, gaining insider information from wearable devices and using it for financial gains, assaulting a smart city through the internet, and performing sex crimes via connected items in the smart home.

Keywords Morphological analysis · Internet of things · Scenario development · Crime · Terrorism · Terrorist attack · Security

Introduction

The Internet of Things (IoT) is a paradigm under which common objects are equipped with sensing, information processing and communication capabilities, and communicate with each other over the internet [1]. While many digital devices like desktop and laptop computers and smartphones are already connected to the internet, the core idea of the IoT is to expand this capability for networking to practically every object which we use: from tiles on the pavement to cars on the street, and from the kitchen sink and smoke detector in our houses right down to the lowly toothbrush and hair comb.

The Internet of Things (IoT) is expected to proliferate widely in the coming decade. According to CompTIA, about 50.1 billion objects will be connected to the IoT by 2020 [2]. Other notable forecasts by respected firms like Morgan Stanley and Huawei state that we will see 75 billion and 100 billion networked devices by 2020 [3] and 2025, respectively [4]. It seems clear that the IoT will become a definite part of our lives in the future, with all the benefits it can confer on us – as well as the risks.

It is common knowledge that criminals and terrorists are early adopters of new technologies [5] – largely because the conventional technologies are already well-defended and highly regulated. Many IT firms are concerned that the IoT is a "security disaster waiting to happen" [2], but few know exactly what to expect, as criminals and terrorists are making their first forays into the open sea of IoT-enabled crime and terror attacks. Security breaches from cloud-based devices are constantly on the rise (with a 152% rise in just 1 year between 2014 and 2015 [6]). The number of cyber-attacks is rising precipitously as well, and since in the future many objects and machinery will be connected to the IoT, the implications are that cyber-attacks can be translated directly from the virtual to the physical world. Terrorists will be able to profoundly

✉ Roey Tzezana
roey@post.tau.ac.il

[1] Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, Tel Aviv, Israel

impact the physical world in other countries, without actually getting up from their chair in front of the computer.

The future of the IoT means that security forces must prepare themselves for new kinds of crime and terrorist attacks. To do that, in this study we have worked with fifty experts on Wikistrat's crowdsourcing platform, and together we have developed a series of scenarios that describe future potential crime and terrorist attacks that utilize and rely on the IoT. The scenarios were developed using General Morphological Analysis (GMA), and were then graded by the experts according to their plausibility. The most plausible scenarios are described in length in this paper, along with lessons and insights about the usability of Wikistrat's platform for collaborative thinking and scenario development.

Scenario development and morphological analysis

There are many methods used to distinguish between different categories of scenarios and scenario development processes [7–9]. In their seminal review of the field, Bishop, Hines and Collins have identified eight general categories of scenario techniques, and more than 23 different techniques used to develop scenarios [10].

Out of all of those, we have chosen to use General Morphological Analysis (GMA) as the technique with which to develop the scenarios. Bishop *et al.* describe Morphological Analysis as a technique that is especially relevant when dealing with dimensions of uncertainty. In their words: "(…)we have to deal with systems in chaos and/or emergent states that are inherently unpredictable" [10].

It therefore seems that GMA is particularly suitable to analyze the possible uses terrorists and criminals will have for the IoT.

The original concept of GMA was born in the mind of astronomer Fritz Zwicky in 1948 [11]. The method was later utilized widely and disseminated by Tom Ritchey of the Swedish Morphological Society. Ritchey has also added layers of sophistication and capabilities to the method by developing a computerized system for automated analysis and cross-consistency assessment (CCA) functions [12–14]. GMA has been widely used in many different fields, from design to policy analysis [15]. In security and defense studies, in particular, it has been used recently to evaluate preparedness for HAZMAT accidents [16], to create threat and sabotage scenarios for nuclear facilities [17], and to outline a framework for proactive risk management in civil aviation [18].

Morphological analysis is conducted by identifying several categories of *factors* that influence the final scenario, and which are grouped into different categories called *parameters*. The factors are then cross-matched to produce *kernels* (as Bishop *et al.* eloquently put it) for scenarios that can then be more fully developed.

We have made use of GMA on Wikistrat's crowdsourcing platform, to produce novel scenarios describing how criminals and terrorists could use the IoT in the near future to accomplish acts of crimes and terror. Fifty experts in cyber-security and other fields have meshed together different factors from three categories: *targets*, *motives*, and *methods*. They then ranked each factor according to its likelihood or impact. A typological field was created containing 9,660 combinations of factors – each of which being the basis for a scenario to be developed. We have also expanded on three combinations of high impact and high likelihood, and on three combinations of high impact but low likelihood (the 'wild cards') and developed scenarios around them, which were then reflected upon, edited in a highly collaborative crowdsourced fashion, finalized and graded according to their plausibility.

Wikistrat's crowdsourcing platform

Wikistrat is a crowdsourcing consulting company that utilizes the 'wisdom of experts' on a crowdsourcing online platform. The platform is similar in style and looks to Wikipedia, and enables experts to easily discuss issues with each other, collaborate on scenario development and vote on various questions. The participants can openly share information and knowledge with each other, correct each other's mistakes and work together to improve their ideas [19]. These properties make Wikistrat's platform ideal for conducting brainstorming and developing ideas and scenarios in large groups of dozens of experts.

The platform has been described in at least one review as facilitating "faster synthesis and analysis amongst analyst teams" and enabling multiple teams to work in parallel while still being exposed to each other's work and benefiting from it [20].

Wikistrat has a community of over 2,500 experts and analysts that come from a variety of backgrounds, and the company verifies each expert's background before he or she is allowed to enter the community and take part in ongoing research. For the current research, we sent an invitation to Wikistrat's community, and the experts self-selected themselves by taking part in the discussions. Altogether we had fifty experts in the discussions and voting sessions. Out of those fifty, 33 had knowledge and background in security, cyber-security or antiterrorism. The others had various backgrounds, mostly in the social sciences. We believe that this diversity is crucial in any effort to create scenarios that combine both understanding of novel technologies like the IoT, and their potential impact on nations, governments and citizens.

Methodology

We conducted the research in the following three steps:

1. Factors Identification: we identified 6–9 factors in each category of *methods*, *motives* or *targets*.
2. Scenario Development: the experts were asked to match together any three of the factors – one from each category – and to develop scenarios that depict ways in which criminals and terrorists utilize the IoT for their purposes.
3. Determining Plausibility: the experts were asked to grade each scenario according to its plausibility.

Each step is presented in detail in the following sections.

First step: identifying factors

The factors were identified in previous research (unpublished as yet) by the same experts, and ranked according to their impact and likelihood. We selected between six and nine factors in each category, and those factors were presented to the experts in the second step.

Second step: scenario development

The factors were presented to the experts, who were then asked to match them together and develop plausible scenarios for future crime and terrorist acts relying on the IoT. The experts were encouraged to work together, to give feedback about each other's scenarios and even 'barge in' and rewrite scenarios written by their colleagues. This part of the research only took 4 days – a time that has been found to be optimal in similar research conducted in the past on Wikistrat's platform, to ensure that the experts' attention is kept at a maximum.

Third step: determining plausibility

The scenarios were ranked by the experts according to their plausibility. The final plausibility score for each scenario was calculated according to the following formula –

$$Plausibility\,Score = \frac{(1*N_1) + (2*N_2) + (3*N_3)}{N_{all}}$$

With N_1, N_2, N_3 being the numbers of participants who voted for *low*, *medium* or *high* plausibility, respectively. N_{all} is the total number of participants who took part in the rankings for each scenario.

Results and discussion

Factors identification

A total of nine factors in the *motives* category, eight factors in the *targets* category and five factors in the *methods* category were selected for the next phase (see Table 1). Since some of the participants were not experts in cyber-security and did not understand some of the methods suggested by their peers, we added a sixth generic method – "Genius Hacker" – basically a 'joker' that does not have to be explained any further. The analysts could use that method as a generic catchphrase to describe a crime or a terrorist act which they could not explain otherwise how it would be performed.

Scenario development

The experts worked together to create 24 scenarios. Three of the scenarios ended up being redundant, and some of their ideas were combined with other similar scenarios, for a final count of 21 finished scenarios.

The experts provided constant feedback for each other's work. Each scenario received anywhere between zero and ten comments, with the median number of comments for each scenario being 4. The median number of revisions for each scenario, including revisions by the original author and by other participants, was 3. These results indicate that the experts were indeed involved in each other's work, consulted each other, provided feedback and made corrections in their writings. It is also likely that some experts exchanged private

Table 1 The lists of factors, which the experts in the study used to develop their scenarios

Motives	Targets	Methods
Blackmailing	Automobile Sensors and Controls	A "Genius Hacker"
Damaging the reputation	Cyberwallets	An "Inside Man"
Deep surveillance	Hospitals and Health Facilities	Botnets
Identity theft	Intelligence and defense information systems	DDoS
Industrial espionage	Nuclear and Energy Power Plants, Electrical Grids, and Pipelines	Mass Attack by Thousands of Computer Users
Political subjugation and control	Smart Assistants	Social Engineering
Propaganda	SmartHome Platforms	
Sex crime	Traffic management systems	
Surveillance and exposure of the intelligence community		

messages on the platform concerning the scenarios, but such private discussions were not monitored for obvious reasons.

Determining plausibility

Following the scenario development process, the experts ranked each scenario according to its perceived plausibility. The final results appear in Table 2, along with a brief description of each scenario.

In-depth scenario analysis

While an in-depth analysis of all the scenarios had been conducted as part of the research, this paper's constraints allow us only to focus on the four most plausible scenarios, present evidence for their feasibility, and explain their significance.

Smart home blackmailing

In this scenario, the IoT appliances in smart homes allowed criminal hackers to spy on the lives of private citizens and blackmail them using sensitive material. Such crimes seem highly likely in light of the common use of ransomware in the present, especially ones tapping into webcams [21]. Similar ransomware that could tap into the smart house appliances and record the victims could be used to blackmail people in the near future as well.

This scenario is based on the fact that smart homes are rapidly turning from an abstract concept to a reality. IoT devices can be found everywhere, and include smart door locks,[1] virtual assistants like Amazon Echo,[2] smart baby monitors and security cameras,[3] smart thermostats,[4] and even smart grills[5] and household robots.[6] All of the above can be connected to the internet and be controlled by their owners via dedicated apps or platforms. They can also be hacked, as has already been demonstrated in 2016, when inherent flaws in Samsung Smart Home platform allowed hackers to control people's light bulbs and even door locks with ease [22]. By the time the flaw was discovered, the system was already installed in at least a hundred thousand homes (according to the number of downloads of the app in the Google Play Store).[7]

Insider information

In this scenario, a wealthy business man's wearable devices are hacked by criminals, and used to gather information about that person's financial decisions. Criminals and crime organizations that manage to conduct such attacks successfully could remain unknown and unseen for a long time, while getting consistently richer by means of their insider information.

This scenario seems especially likely since sophisticated emerging technologies like wearable devices and smart home appliances and platforms are often being used by the wealthy before they become everyday utilities. As a result, these technologies are not as secure as they should be in their early stages. Wealthy individuals could easily find themselves under surveillance by criminals who will break into their IoT devices and track and record their every movement and doings.

Smart city under attack

The participants highlighted two potential highly-plausible scenarios relating to cyber-attacks on smart cities:

- Cyber-attack as a precursor to a physical attack: a highly capable terrorist group could remotely conduct a cyber-attack to essentially shut down or disrupt the ongoing affairs of a city. The cyber-attack would then enable and be followed by a more conventional attack enacted by terrorists with guns or explosives.
- Cyber-hacktivists disrupting city functions: cyber-hacktivists would shut down or disrupt some key infrastructure units in a smart city, leading to political embarrassment, economic damage and potentially even loss of human lives. Such incidents can be particularly expected during an important and highly visible political, sporting or economics event stage in the city.

Additionally, the analysts indicated that two of the top-impact targets for shutting down a smart city would be the traffic management systems and the electrical grid, which includes an actual disruption of the workings of nuclear and energy power plants.

Smart cities are beginning to form around the world. Nicolas Reys, in his report for the ControlRisks consultancy, explains that they are the natural outcome of three technologies being combined together: cheap logic controllers, a large number of sensors spread all over the city, and a network that connects them all together. Several cities are well on their way towards becoming 'smart', including Amsterdam, Barcelona, Santa Cruz and Stockholm [23].

[1] http://august.com/. Accessed 03 July 2016

[2] https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/. Accessed 03 July 2016

[3] http://www.withings.com/us/en/products/home. Accessed 03 07 2016

[4] https://nest.com/thermostat/meet-nest-thermostat/. Accessed 03 July 2016

[5] https://www.amazon.com/iDevices-IGR0009P5-iGrill2-Bluetooth-Thermometer. Accessed 03 July 2016

[6] https://www.ald.softbankrobotics.com/en/cool-robots/pepper. Accessed 03 July 2016

[7] https://play.google.com/store/apps/details?id=com.smartthings.android&hl=en. Accessed 03 July 2016

Table 2 A short description for each of the 21 scenarios the experts developed for crime and terror acts relying on the IoT

Scenario	Final plausibility score	Short description
Smart home blackmailing	2.37	Hackers break into smart homes systems, retrieve information about the house occupants, and use embarrassing information as blackmail material
Insider information	2.37	Wearables and similar IoT appliances are used by criminals to track wealthy individuals and understanding their financial decisions and whereabouts in order to anticipate financial moves in advance
Smart city under attack	2.33	A highly capable terrorist group combines a cyber-attack on infrastructure in a smart city with a physical attack with guns and explosives
Sex and the smart home	2.33	Smart home platforms are used to record and steal sex-related videos and images
Killer traffic	2.31	A hacker shuts down traffic intersections in a smart city, by making the traffic lights show red on all sides, or even showing green on all sides. When the locations where the lights failed are connected by lines on Google Map, the personal name of the perpetrator of the hack appears.
Open cyberwallets	2.29	Crime organizations hack into IoT devices that receive payment from cyberwallets, and gather an incredibly large amount of data about millions of individuals
Defense systems puppeteering	2.28	Military information gathering systems are hacked so that the attackers can actively use them to collect information on items of their choice
Killing hospitals	2.27	Terrorists shut down the power to multiple hotels in one city, by manipulating the smart grid in the city and the hospitals. Their purpose is to cause maximal damage in life. Thousands of patients undergoing surgery find themselves under threat
Damaging a hospital's reputation	2.24	Competing health services utilize DDoS attacks to hinder the functions of targeted hospitals, thus damaging their reputation in the eyes of the public
Financial terrorism	2.23	Criminals and/or terrorists use botnets to attack and control IoT devices like smartphones that are used to execute and manage financial transactions, aiming to disrupt the financial system
Attacking cyberwallets	2.17	A crime organization targets a single brand of retail stores and takes down their devices that enable payment via cyberwallets. The attackers will only stop for a blackmailing fee - which will probably be cheaper for the company to pay, rather than wait for its experts to deal with the hack in real time
Agent recruitment	2.15	Wearables and smart home platforms could be used by foreign powers / crime organizations / terrorist groups to gather information about potential agents and to recruit them
Smart and vulnerable	2.15	Hackers break into smart homes systems, retrieve information about celebrities or politicians in the house, and release the information to embarrass them or gain political leverage
Terrorists just love to show off	2.14	Terrorists enact many DDoS attacks simply so that they remain 'in the news' and create an atmosphere of fear and helplessness
Supply chain under threat	2.12	Industrial adversaries break into each other's sensors networks located throughout their supply chains, to gather knowledge about their operations and possibly disrupt them
Steal resource data	2.10	Nation-sponsored agents, terrorists or crime organizations will break into systems that collect data about resources (oil, rare earth elements, etc.) in order to understand where best to attack and gain knowledge about the processing technologies for those materials
Marketing assistants	2.02	Crime organizations or firm-sponsored criminals will infiltrate smart assistants to manipulate customers' preferences in purchases
Taking the grid down	2.02	A coordinated mass attack on power grids and power plants brings down a large part of the grid, and leaves millions without electricity
Leaks all around	2.00	Hacktivists will use IoT devices to collect as well as disseminate information about governmental operations, in a similar fashion to what Wikileaks is doing

Table 2 (continued)

Scenario	Final plausibility score	Short description
Political assistants	1.86	Smart assistants are infiltrated so that they influence users in political ways - for example, by mostly showing news of a certain political orientation
Blackmailing a nation	1.71	The attackers take control over key utility infrastructure, and blackmail the citizens themselves in order to provide access to the services

Sex and the smart home

Sex crimes could be enacted by relying on the IoT. Examples for IoT-based sex crimes, outlined by the analysts, include –

- Sexual assault: by gathering information from smart home appliances about the victim's whereabouts and habits, the attacker could know exactly when and where to strike.
- Obscenity (communicating sexual meaning to the victim): by using IoT speakers, the offender could broadcast obscene sexual messages to people, including children (as may already have happened when hackers took control of IoT-connected baby monitors and used them to chat with babies in their cribs) [24].
- Exhibitionism (displaying sexual content to a victim for pleasure): similarly to *obscenity*, the offender could use connected speakers and/or TV sets in other people's houses to enact an exhibitionism crime on a scale unrealized before.
- Voyeurism (observing others for a sexual motive): by hacking into the various appliances in the smart home, the offender could spy on the inhabitants sexual or daily activities for his or her sexual relief.

In addition, one of the most plausible scenario described by the analysts was that in which an offender stole sex-related amateur videos recorded in people's homes or hotels. The videos could either have been recorded intentionally by the inhabitants themselves, or by the hacker controlling their home cameras and microphones. These videos could be used for blackmail purposes or even for political gains in cases where high-caliber political actors are recorded.

It should be noted that similar cases have happened before, for example in the case of Miss Teen USA whose webcam had been hacked into, and used to take her nude photos in her bedroom. The offender was only discovered when he tried to blackmail the victim and force her to send him more nude photos [25]. He had been arrested, along with 97 other offenders who hacked into victims' webcams to spy on them remotely, using software commercially sold for less than $170 [26]. While in these cases the offenders hacked into their victims' computer webcam, similar crimes can be expected to occur using IoT devices as well.

Conclusions

The IoT holds great potential to make a positive impact on the world, but it also makes us highly valuable to cyber-attacks. As Marc Goodman wrote, "when everything is connected, everyone is vulnerable" [27]. The digital world is filled to the brim with digital criminals, hackers, virus programmers, ransomware spreaders, hacktivists and all possible kinds of people who skirt on the edge of the law at best, or violate it completely at worst. As we connect our things to the internet, we will give all of the above access to our critical infrastructure, our houses and even our bodies.

In this research we created a list of scenarios, ranked by plausibility, that describe novel ideas for acts of crime and terror that rely on the IoT. We described in length the four most plausible scenarios and have shown that they are indeed highly likely – and some have already began happening in some preliminary versions.

While we do not believe that these 21 scenarios can even come close to describing the full use that criminals and terrorists will make of the IoT, we see this paper as a starting point for more in-depth research on the issue. Hopefully, such research will shed more light on this urgent issue, and will serve to warn governments, private companies and individuals of the dangers ahead of time.

Acknowledgements The author wishes to thank Wikistrat executives Dr. Shay Hershkovitz, Oren Kesler and Nick Ottens who authorized the use of Wikistrat's platform for the purposes of the research and helped design the research methodologies and manage the participants. Special thanks go to the participants in the research, who willingly contributed of their knowledge and expertise. Finally, the author wishes to thank Tom Ritchey who first introduced him to GMA and gifted him with his book "Wicked Problems, Social Messes" about the methodology.

Compliance with ethical standards

Funding This work was supported by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University.

Declaration of interest The author is a senior analyst in the Wikistrat community.

References

1. Whitmore A et al (2014) The internet of things—A survey of topics and trends. Inf Syst Front 17(2):261–274
2. CompTIA (2016) Internet of things insights and opportunities. CompTIA
3. Danova T (2013) Morgan Stanley: 75 billion devices will be connected to the internet of things by 2020. Business insider, 2 10 2013. [Online]. http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10. Accessed 28 June 2016
4. Hernandez P (2016) IoT to Cover 100 billion connected devices by 2025. Datamation, 13 4 2016. [Online]. http://www.datamation.com/data-center/iot-to-cover-100-billion-connected-devices-by-2025.html. Accessed 29 June 2016
5. Meghraoua L (2016) Criminals have always been early adopters of new technology. Látelier, 16 8 2016. [Online]. http://www.atelier.net/en/trends/articles/criminals-have-always-been-early-adopters-of-new-technology_442892. Accessed 06 Sept 2016
6. Wong JI (2016) Cybercrime is booming and the internet of things will just make things worse. Quartz, 27 1 2016. [Online]. http://qz.com/603996/cybercrime-is-booming-and-the-internet-of-things-will-just-make-things-worse/. Accessed 29 June 2016
7. van Notten PWF (2003) An updated scenario typology. Futures 35(5):423–443
8. Bradfield R (2005) The origins and evolution of scenario techniques in long range business planning. Futures 37(8):795–812
9. Börjeson L et al (2006) Scenario types and techniques: towards a user's guide. Futures 38(7):723–739
10. Bishop P et al (2007) The current state of scenario development: an overview of techniques. Foresight 9(1):5–25
11. Zwicky F (1948) The morphological method of analysis and construction. California Institute of Technology, California
12. Ritchey T (2009) Morphological analysis. In: Glenn JC, Gordon T (eds) Futures research methodology. V3.0. The Millennium Project, New York
13. Ritchey T (2011) Wicked problems - Social messes: decision support modelling with morphological analysis. Springer, Berlin
14. Ritchey T (1998) General morphological analysis - A general method for non-quantified modelling. Swed Morphological Soc 1–10
15. Álvarez A (2015) Applications of general morphological analysis. Acta Morphol Gen 4(1):1–40
16. Ritchey T et al (2002) Using morphological analysis to evaluate preparedness for accidents involving hazardous materials. 4th International Conference for Local Authorities, Shanghai
17. Ritchey T (2003) Nuclear facilities and sabotage: using morphological analysis as a scenario and strategy development laboratory. 44th Annual Meeting of the Institute of Nuclear Materials Management, Phoenix
18. Jimenez H et al (2009) A morphological approach for proactive risk management in civil aviation security. 47th AIAA Aerospace Sciences Meeting including The New Horizons Forum and Aerospace Exposition, Orlando
19. Wikistrat (2015) Wikistrat's analytic tradecraft. Wikistrat
20. Raford N (2014) Online foresight platforms: evidence for their impact on scenario planning & strategic foresight. Technol Forecast Soc Chang 97. doi:10.1016/j.techfore.2014.03.008
21. US-CERT (2013) Recent Reports of DHS-Themed Ransomware (UPDATE). Department of Homeland Security, 30 7 2013. [Online]. https://www.us-cert.gov/ncas/current-activity/2013/07/30/Recent-Reports-DHS-Themed-Ransomware-UPDATE. Accessed 03 July 2016
22. Fernandes E (2016) Security analysis of emerging smart home applications. Proceedings of 37th IEEE Symposium on Security and Privacy, May 2016. https://iotsecurity.eecs.umich.edu/img/Fernandes_SmartThingsSP16.pdf. Accessed 20 Nov 2016
23. Reys N Smart cities and cyber threats, ControlRisks, https://www.controlrisks.com/~/media/Public%20Site/Files/Our%20Thinking/Urbanisation/Smart%20cities%20article.pdf. Accessed 20 Nov 2016
24. Storm D (2015) 2 more wireless baby monitors hacked: hackers remotely spied on babies and parents. ComputerWorld, 22 4 2015. [Online]. http://www.computerworld.com/article/2913356/cybercrime-hacking/2-more-wireless-baby-monitors-hacked-hackers-remotely-spied-on-babies-and-parents.html. Accessed 29 June 2016
25. Shontell A (2014) Miss teen USA was 'In tears and shock' after a hacker took nude photos through her bedroom webcam. Business Insider, 23 5 2014. [Online]. http://www.businessinsider.com/cassidy-wolf-discusses-the-hacker-who-captured-nude-photos-of-her-via-webcam-2014-5. Accessed 03 July 2016
26. Borison R (2014) 97 people arrested for hacking into webcams remotely and spying on people. Business Insider 19 5 2014. [Online]. http://www.businessinsider.com/97-arrested-for-spying-through-webcams-2014-5. Accessed 03 July 2016
27. Goodman M (2015) Future crimes: everything is connected, everyone is vulnerable and what we can do about it. Doubleday