

# Future and Emerging Threats to Network Operation: A Quantitative Research Analysis

(Interim Report, 2<sup>nd</sup> August 2011)

Alberto Schaeffer-Filho and Andreas Mauthe  
School of Computing and Communications  
Lancaster University  
Lancaster, United Kingdom  
{asf, andreas}@comp.lancs.ac.uk

Sally McClean and Gerard Parr  
Faculty of Computing and Engineering  
University of Ulster  
Coleraine, Northern Ireland, United Kingdom  
{si.mcclean, gp.parr}@ulster.ac.uk

**Abstract**—The digital threat landscape on telecommunication and network operations is evolving due to a number of emerging factors. These include social and human factors (social engineering, new applications, and interpersonal trust), new types of devices, applications and end-systems (e.g. iPads, Facebook, e-Banking, iPlayer, etc.), and network and infrastructure vulnerabilities (e.g. network attacks, failures and misconfiguration). In order to understand the impact of future threats to network operations, we have asked a selected group of experts in the area of computer networks for their input. In this report, we present our initial findings based on the information provided by these experts. We were able to capture significant insights into how they perceive the causes, drivers and relevance of future threats to network infrastructures. The information obtained not only highlights the general perceptions and trends from the experts' answers, but also allows us to understand and contrast the answers of respondents from different backgrounds. The full report will be available once the analysis has been completed. This should also contain a comparison between India and UK.

## I. INTRODUCTION

The study of future and emerging threats to network operation is not a popular research topic, as typically we concentrate our efforts on finding solutions for current problems rather than speculating about the future [1]. However, the threat landscape on computer networks has been maturing fast in the last few years. For this reason, it is crucial that we improve our understanding of the vulnerabilities of the critical infrastructure underpinning the future Internet. We advocate that in order to anticipate future threats and how they can affect the network, infrastructure and services, we need first to understand how current networks can be affected by a series of emerging impact factors. We expect that this will help us to explore the space of future threats in networking in a more systematic manner.

We are currently looking into emerging and future threats to network operations caused by various factors, ranging from

social and human factors (such as social engineering, new applications, and interpersonal trust), over new devices, applications and end-systems (e.g. iPads, Facebook, e-Banking, iPlayer, etc.), to network, systems and infrastructure factors (e.g. network attacks, failures and misconfiguration). In order to understand how these factors might impact the operation of future networks, we designed an extensive questionnaire, distributed it to selected groups of experts in the area of computer networks, and asked for their input. Through this questionnaire we were able to capture significant insights into how experts perceive the causes, drivers and relevance of future threats to vital networks and communication infrastructures.

In this report, we present our initial findings and draw a number of conclusions on the impact of future and emerging threats to network operation. The way the questionnaire was designed not only permitted us to obtain information on the general perceptions and trends from the experts' answers, but also to understand and contrast the answers of respondents from different backgrounds. These results enabled us (1) to analyse the perceived vulnerabilities of critical telecommunication infrastructures, (2) to contrast the perceptions from industry, academia and government, and (3) to identify research priorities within each context. The full report will be available once the survey has been closed and a full analysis has been carried out on the complete data set. This should also contain a comparison between India and UK.

This work is in line with recent strategic studies developed by the UK Government about actions and recommendations to ensure the leading role of the UK in the global digital economy [2]. These recommendations highlight that most of the risks of the real world also exist in the digital world, including dissemination of harmful or offensive material, lies, scams, invasion of privacy, as well as physical attacks. In addition, there is the risk of attacks to critical system. Despite these issues, a recent study ranked the UK last in terms of the level of involvement between executives of critical infrastructure companies and their governments on tackling cyber security issues [3]. We expect that our findings will be

This work is led by Lancaster University and being conducted as part of the India-UK Advanced Technology Centre (IU-ATC) consortium. The IU-ATC is funded by the UK Government through the EPSRC and by the Indian Government's Department of Science and Technology (DST).

able to provide additional inputs into the government strategy and cyber security policy development.

This report is organised as follows: Section II discusses a number of emerging impact factors that we believe will shape the threat landscape on the future Internet. Section III describes our methodology, including the overall structure of the questionnaire and the profile of the respondents. Section IV presents the first set of results in terms of the general perceptions obtained from the whole set of respondents. Section V presents our results cross-tabulated by the respondents' job area, in order to draw conclusions about the perceptions within each specific context. Finally, Section VI outlines the concluding remarks.

## II. EMERGING IMPACT FACTORS

The digital threat landscape has been maturing fast in the last few years. We have identified a range of *impact factors* that we believe are likely to shape the form of emerging threats in the future Internet. In this section, we briefly discuss the possible implications of these impact factors. These were used in the design of the questionnaire that was answered by experts in the area. Their perceptions and opinions on future and emerging threats to the network operation are analysed and presented in the remaining part of this report.

### A. Motivation and Goals of Adversaries

In order to anticipate emerging threats one needs to understand the adversaries, their motivation and goals. These have been shifting from recreational hacking, to hacking as a form of financial gain. More recently, the term "hacktivism" [4] has been used to describe a non-violent cyberattack in pursuit of political ends, which can be seen as the cyber equivalent of "protesting". The tools and methodologies are similar to those used in other types of attacks, but differently from recreational hacking or hacking for profit, "hacktivism" tends to be driven by political events.

Recent developments escalated the possibility of using hacking as a military/political weapon, e.g. the cyberwar in Estonia [5], which consisted predominantly of defacement of government websites and distributed denial of service attacks. Similar attacks occurred against a number of Georgian government websites in August 2008 during the armed conflict between the Russian Federation and the Republic of Georgia, as well as cyber attacks against both Israeli and Palestinian websites following the Israel invasion of the Gaza strip in January 2009 [4].

### B. New Technologies

The introduction of new types of applications, services and devices must be considered as a potential cause of technical challenges in the network: for example, the recent claims that the iPad broadcasts its Wi-Fi signal at higher power levels and may disrupt other devices [6]. Additionally, new attack vectors based on cloud computing and virtualisation are also likely to emerge. Servers in the cloud are moving outside the security boundaries of a company or data centre and may be co-located

with potential malicious servers [7]. In this situation, attackers might use standard botnets to affect the availability of cloud resources. Likewise, data in the cloud is also at risk of being stolen or tampered with.

Modifications in current established Internet protocols are also likely to stimulate new forms of attacks. In particular, as IPv6 becomes more popular and more users adopt the protocol, its weaknesses will be discovered similarly to what occurred with IPv4. Similarly, modification in the DNS and the introduction of international characters (Russian, Chinese, Arabian, etc) into domain names might create new possibilities for old attacks, such as phishing based on malicious domains having similar-looking names to their legitimate counterparts [7].

### C. Social Engineering Methods

While the intrinsic nature of malware software and attacks has not changed much in the recent years, the real changes are in the ways malicious code is written, to make these attacks more stealthy and difficult to detect and resistant to analysis [1]. At the same time, old forms of attacks may benefit from the recent development of social engineering methods. Social engineering [8] can be seen as a social/psychological process through which someone can persuade and obtain sensitive information from others in order to enable a further attack. Recently, social networking websites have been increasingly misused for gaining sensitive information, for financial profit or to discredit a person, company or institution [9], [10]. Social networks raised concerns about personal data security, including identity frauds, data theft, dangers from hackers and viruses.

### D. System Complexity and Scale

Communication networks, the backbone of the future digital economy, are becoming increasingly more complex and thus more vulnerable, incurring on scalability problems, dependencies and cascading faults. This complexity also lend communication networks more susceptible to human mistakes [1]. Ultimately, disruptions in parts of the system may result in the collapse of the whole network due to complex interdependencies.

### E. Mobility and Constrained Devices

While global attacks are becoming less frequent, localised attacks are expected to increase [7]. Attacks seeking for financial gains have been typically targeted at personal computers because this was where sensitive user data could normally be found. However, recent advances in the mobile technology industry and its widespread adoption mean that smartphones are more likely to become the new target for cybercrime [7].

Increasing use of mobile devices associated with their limitations in battery and processing power make the use of conventional security solutions impractical. File scanning, system call monitoring and packet analysis are all too heavy-weight mechanisms and consume a large amount of battery power. This makes likely that both vendors and consumers will trade security for more battery life [11].

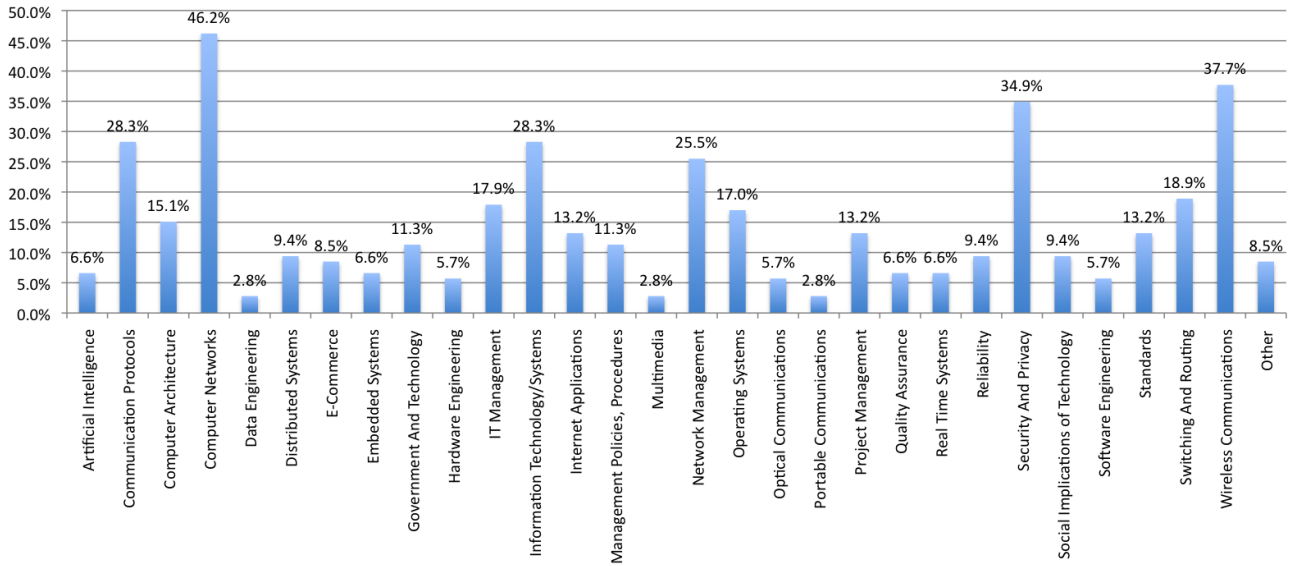


Fig. 1. Profile of respondents per expertise.

### F. Regulation and Accountability

Different countries and organisations have their own regulatory measures, accountability and law enforcement policies, and the lack of standard procedures will make the adoption of new security and resilience solutions increasingly difficult. Moreover, the identification of attacks requires cross-border communication which is time-consuming, bureaucratic and prevent the prompt reaction to attacks [1]. For example, the UK Government advocates that the Internet governance must be considered and shared at three levels in order to minimise its risks [2]: *global level*, concerning the cross-jurisdiction nature of networks, *national level*, to address issues that are more appropriately dealt by national actions, and *consumer level*, by enabling all individuals to protect themselves. The interactions between these three levels require the clear definition of policies, standards and legal frameworks.

## III. METHODOLOGY

Based on these emerging impact factors, we designed an online questionnaire and asked experts in the area to provide their perceptions on the topic. The questionnaire consisted of 31 questions (both quantitative and qualitative) divided into 5 main sections: (i) perceptions on future and emerging threats, (ii) classification of threats to the future Internet, (iii) future and emerging network anomalies, (iv) prevention, evaluation and planning, and (v) personal background. In particular, personal background questions were used to obtain details about the respondent's job title, area of expertise and country. This allowed us to cross-tabulate results and compare answers of respondents from research and industry, for example. Similarly, the data permitted the comparison of

the perceptions by respondents from different countries<sup>1</sup>.

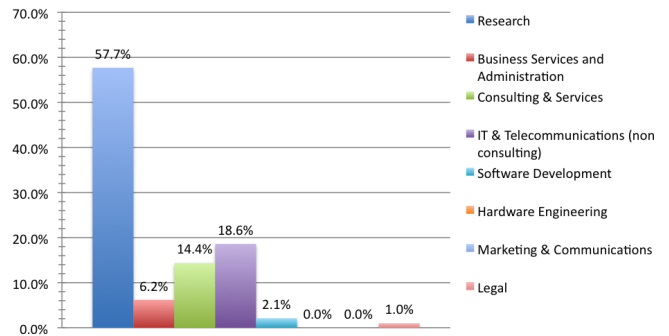


Fig. 2. Profile of respondents per job area.

The questionnaire was sent to a number of specialised mailing lists including several IEEE lists, relevant BCS lists and to a forum of security experts in India. Participants in the study included lawmakers and senior industry figures such Head of Security of one of Europe's largest network operators. Heads of relevant government departments also participated in the study. The questionnaire was responded by a total of 160 people between November 23<sup>rd</sup> 2010 and April 5<sup>th</sup> 2011. Among these, 106 individuals fully completed the questionnaire (66.2%). In the results presented in this report we included only the questionnaires that were answered completely, in order to avoid possible distortions in the analysis caused by partial answers.

The survey is still open and more responses from experts are being collected. At the date of publication, the questionnaire

<sup>1</sup>We are interested in comparing the answers of respondents from the UK and India as part of our future work. We focus our analysis on these two countries alone because the IU-ATC project aims to identify areas of collaboration and synergy between UK and India, as well as to understand the specific needs of each country.

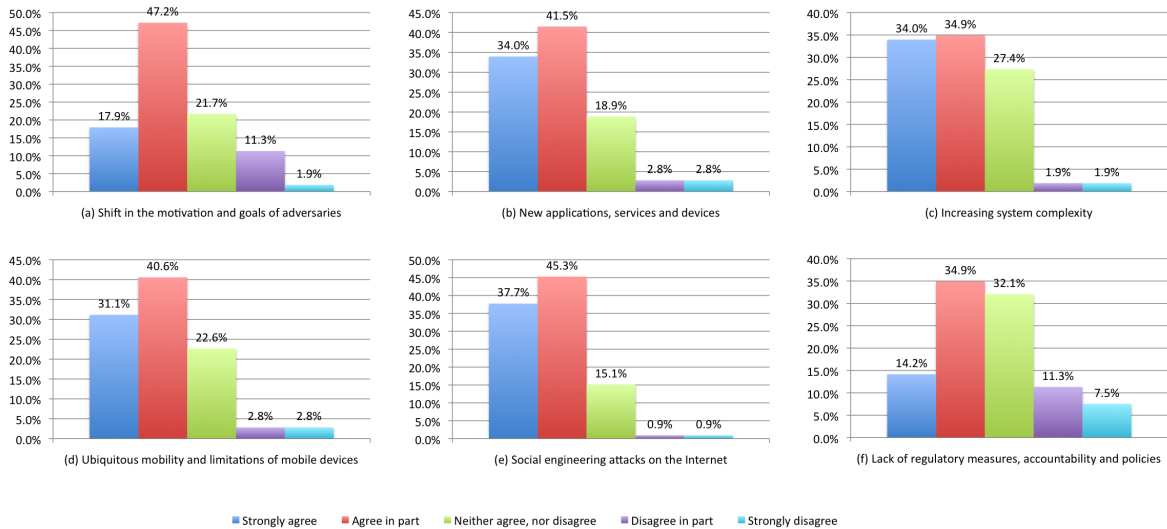


Fig. 4. Possible drivers of the future threat landscape in the next five years

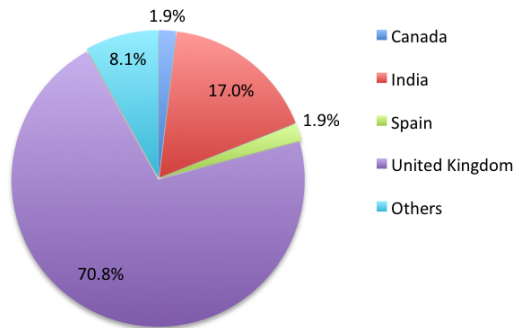


Fig. 3. Profile of respondents per country.

was responded by a total of 238 people, and among these 163 fully completed it. These will become part of the full analysis, which will be presented together with a comparison between India and UK as part of our future work.

Fig. 1 shows the profile of respondents per area of expertise. The three most common areas of expertise among the respondents are computer networks (46.2%), wireless communications (37.7%) and security and privacy (34.9%).

Fig. 2 shows the profile of respondents per job area. It can be observed that 57.7% of all the answers come from research, 35.1% come from IT/telecommunication companies/consulting/hardware and software development, and 7.2% from business service/administration/regulators. Finally, Fig. 3 shows the profile of respondents per country. Most of the answers come from the United Kingdom (70.8%) and from India (17.0%).

#### IV. GENERAL PERCEPTIONS

In this section, we report on the results describing the general perceptions on future and emerging threats to network operation. Due to space constraints, only part of our set of

results is presented, and we concentrate on the most interesting findings of the survey. Note that the aggregate results presented in this section do not yet consider the differences by job area; instead, cross-tabulated results will be presented in the next section.

Fig. 4 illustrates the respondents perceptions about the drivers of the future threat landscape within the next years. Respondents were asked to rate how much they agree or disagree with each one of a series of factors as being a driver of the threat landscape. Even though (as it was expected) the majority of respondents agreed to some extent with most of the factors, these results show that in particular cases the rate of uncertainty (neither agree, nor disagree) is considerably high. This is mostly clear with respect to the *increasing system complexity* and the *lack of regulatory measures, accountability and policies* factors. Moreover, it is interesting to observe that *lack of regulatory measures, accountability and policies* is also the factor considered to be the least likely to cause changes in the threat landscape.

Respondents were also asked to explicitly rank a number of threats to network operation according to their likelihood (1 - most likely, 6 - least likely). The weighted rank is presented in Table I, which includes the percentage of respondents that ranked each threat category the most likely to occur<sup>2</sup>.

Next, respondents were asked to rank a number of factors as possible inhibitors or fears that create difficulties for the acceptance of online/Internet services by the general public. The weighted rank is presented in Table II, which also includes the percentage of respondents that ranked each factor the most likely to be an inhibitor or fear<sup>3</sup>.

<sup>2</sup>Participants were allowed to rank more than one threat as #1, and for this reason the sum of percentages of threats ranked as the most likely exceeds 100%.

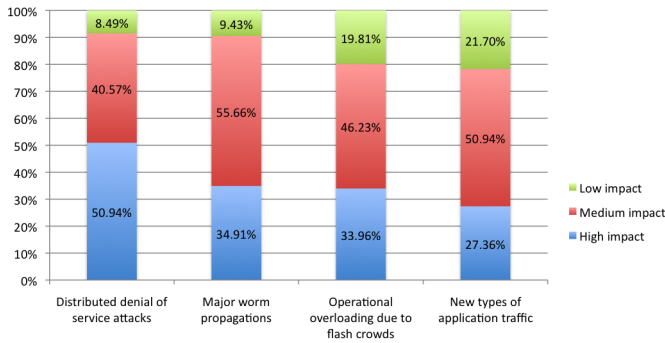
<sup>3</sup>Participants were allowed to rank more than one factor as #1, and for this reason the sum of percentages of factors ranked as the most likely exceeds 100%.

TABLE I  
WEIGHTED RANK OF MOST LIKELY THREATS TO NETWORK OPERATION

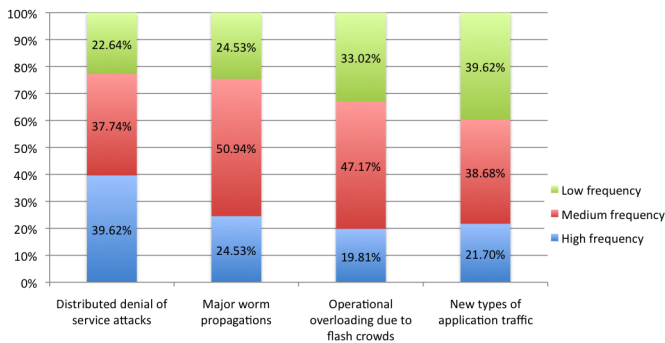
Rank	Description	% most likely
#1	Exploitation of human factor (trust relationships) misusing personal information (e.g. Facebook, e-Banking)	32.08%
#2	Malicious network traffic attacks	27.36%
#3	Vulnerabilities in cloud computing	17.92%
#4	Unforeseen traffic load due to new types of applications (e.g. BBC iPlayer) and devices (e.g. smartphones)	14.15%
#5	Increasing system and network management complexity	9.43%
#6	Physical attacks to the infrastructure	8.49%

TABLE II  
WEIGHTED RANK OF MOST LIKELY INHIBITORS OR FEARS FOR THE ACCEPTANCE OF ONLINE/INTERNET SERVICES BY THE GENERAL PUBLIC

Rank	Description	% most likely
#1	Misuse of personal data and impersonation (Spoofing, Repudiation, Elevation of privileges)	50.94%
#2	Data leakage and privacy concerns (Information disclosure)	47.17%
#3	Lack of security and data integrity on the network (Tampering)	32.08%
#4	Unavailability of the services when they are needed (Denial of service)	20.75%



(a) Impact of traffic issues on the operation of future networks

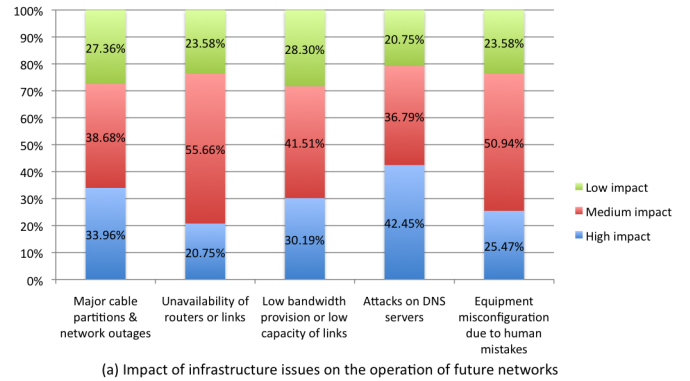


(b) Frequency of traffic issues on the operation of future networks

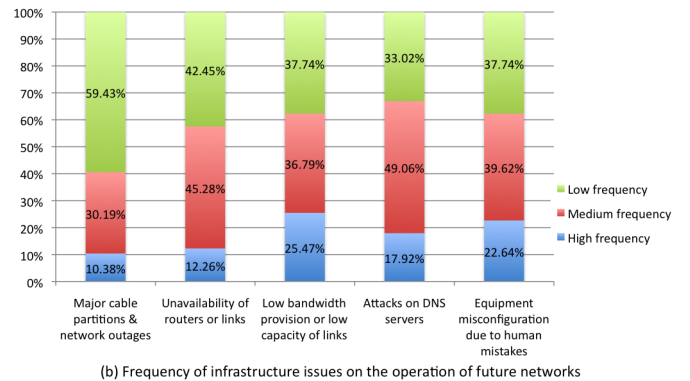
Fig. 5. Perceptions in terms of the impact and frequency of traffic issues on the operation of future networks

Fig. 5(a) and Fig. 5(b) show the perceptions of the respondents in terms of the impact and frequency of traffic issues

in future networks. It can be seen that *distributed denial of service attacks* are regarded as having the highest impact and frequency amongst all traffic issues. Similarly, *major worm propagations* are also regarded as having a high impact and frequency. Finally, *operational overload due to flash crowds* and *new types of application traffic* are regarded as having considerable lesser impact and frequency in future networks.



(a) Impact of infrastructure issues on the operation of future networks



(b) Frequency of infrastructure issues on the operation of future networks

Fig. 6. Perceptions in terms of the impact and frequency of infrastructure issues on the operation of future networks

Fig. 6(a) and Fig. 6(b) show the perceptions of the respondents in terms of the impact and frequency of infrastructure issues in future networks. It can be seen that *attacks on DNS servers* are regarded as having the highest impact, but *low bandwidth provision or low capacity links* is expected to be the most frequent. Also, *unavailability of routers or links* is not regarded as having a high impact or frequency. Finally, *major cable partitions and network outages*, despite having the lowest expected frequency, is still expected to cause a relatively high impact.

Finally, respondents were also asked to indicate what they think will be the most effective strategies in the evaluation of resilience in future networks. The rank is presented in Table III, which includes the percentage of respondents that indicated a strategy as the most effective. *Stress tests on real testbeds* was indicated by the 47.7% as the most effective evaluation strategy. Following that came *metrics and measurement analysis*, *predictive data analysis*, and *multi-layer data correlation and visualisation*, with 35.85%, 28.30% and 21.70%

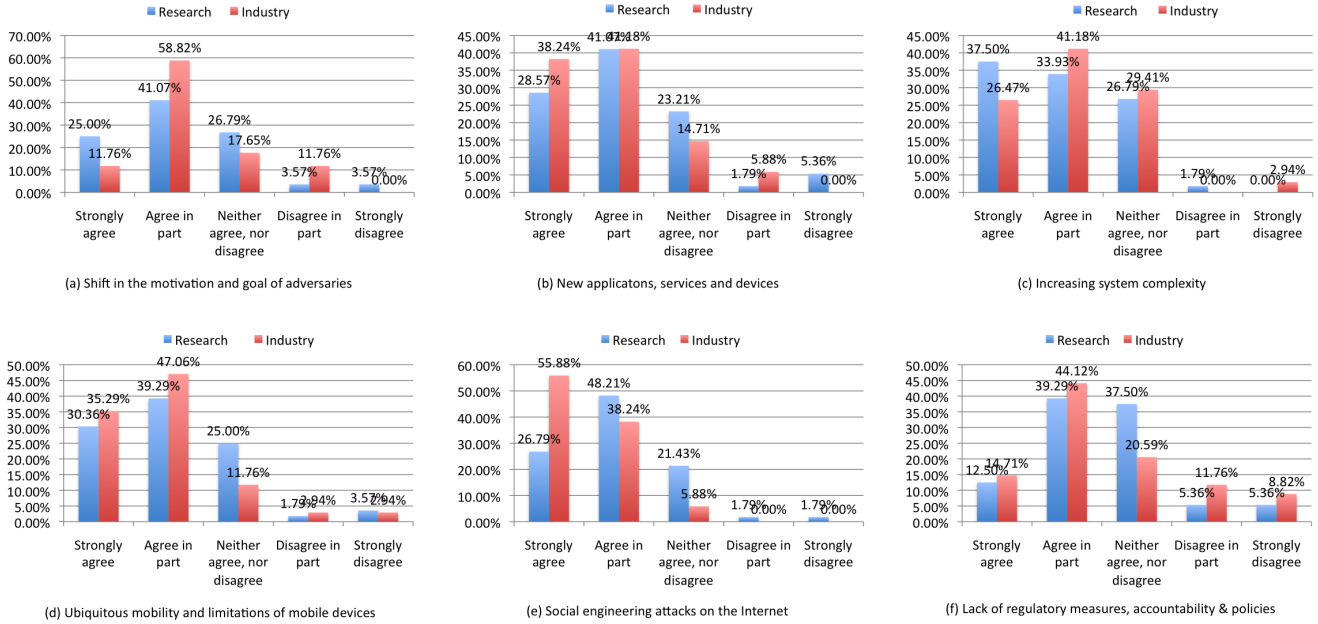


Fig. 7. Possible drivers of the future threat landscape in the next five years according to job area

of people indicating them as the most effective evaluation strategy, respectively. Lastly, *simulation studies* were indicated by only 18.87% respondents as the most effective evaluation strategy.

TABLE III  
RANK OF MOST EFFECTIVE STRATEGIES IN THE EVALUATION OF  
RESILIENCE IN FUTURE NETWORKS

Rank	Description	% most effective
#1	Stress tests on real testbeds	47.17%
#2	Metrics and measurement analysis	35.85%
#3	Predictive data analysis	28.30%
#4	Multi-layer data correlation and visualisation	21.70%
#5	Simulation studies	18.87%

## V. CORRELATED ANALYSIS: CROSS-TABULATION BY JOB AREA

In this section we present a correlated analysis taking into account the respondents' job area. In particular, we compare the differences in perceptions from two groups, namely respondents from research and respondents from industry (the latter including answers from IT/telecommunication companies/consulting/hardware and software development sectors). We expect that these results will help us to better understand the different perspectives and priorities of these groups of professionals.

Fig. 7 illustrates the respondents perceptions about the drivers of the future threat landscape within the next years, according to their job area. Respondents were asked to rate how much they agree or disagree that each one of a series of factors will contribute to the changes in the threat landscape. Although for some factors the differences in perceptions cannot be easily established yet, it is still possible to identify significant trends.

For example, in terms of *shift in the motivation and goals of adversaries* (Fig. 7(a)), whereas the majority of respondents tend to agree in part (41.07% and 58.82% of respondents from Research and Industry respectively), respondents from Research tend to strongly agree more with this factor and at the same time Industry respondents disagree more. Considering *new types of applications, services and devices* (Fig. 7(b)), Industry respondents seem to strongly agree more (38.24% against 28.57%) and conversely Research respondents seem to strongly disagree more (5.36% against 0%). An opposite trend was identified for *increasing system complexity* (Fig. 7(c)), in which the majority of Research tend to strongly agree more (37.50% against 26.47%) and conversely Industry respondents seem to strongly disagree more (2.94% against 0%). A more clear contrasting view can be observed for *ubiquitous mobility and limitations of mobile devices* (Fig. 7(d)), where the rate of respondents from Industry that strongly and partially agree is considerably higher among respondents from Industry than respondents from Research. By far, *social engineering attacks on the Internet* is regarded as the biggest threat among Industry respondents, in which 55.88% strongly agree (against only 26.79% participants from Research who strongly agree). Finally, the *lack of regulatory measures, accountability & policies* is perceived with great uncertainty by Research respondents, whereas Industry respondents tend to agree more (although the rate of respondents from Industry that disagree more is also higher compared to respondents from Research).

We ranked a number of threats to network operation according to their likelihood (1 - most likely, 6 - least likely) individually by job area. This might help for example in the identification of perceived priorities within each context. The weighted rank is presented in Table IV, which includes the percentage of respondents that ranked each threat category

the most likely to occur<sup>4</sup>. These results clearly show the differing perceptions of future threats among the two groups of professionals: while *malicious network traffic attacks* is perceived as the biggest threat among professionals from Research, indicated by 35.71% respondents as the most likely to occur in future networks, it ranked only fourth in Industry considering the weighted rank, although having a high percentage of respondents from Industry indicating it as the most likely threat (20.59%). Conversely, *exploitation of the human factor and misusing of personal information* was ranked first in Industry, with 41.18% respondents indicating it as the most likely threat, whereas it is considered second in the UK, with 26.79% respondents indicating it as the most likely threat. Another interesting observation is that *physical attacks to the infrastructure* ranked last among professionals of both areas, being indicated as the most likely threat by only 8.93% and 8.82% respondents from Research and Industry, respectively.

TABLE IV  
WEIGHTED RANK OF MOST LIKELY THREATS TO NETWORK OPERATION  
ACCORDING TO JOB AREA

Rank		Description	% most likely	
Research	Industry		Research	Industry
#1	#4	Malicious network traffic attacks	35.71%	20.59%
#2	#1	Exploitation of human factor (trust relationships) misusing personal information (e.g. Facebook, e-Banking)	26.79%	41.18%
#3	#2	Vulnerabilities in cloud computing	16.07%	14.71%
#4	#3	Unforeseen traffic load due to new types of applications (e.g. BBC iPlayer) and devices (e.g. smartphones)	17.86%	11.76%
#5	#5	Increasing system and network management complexity	8.93%	14.71%
#6	#6	Physical attacks to the infrastructure	8.93%	8.82%

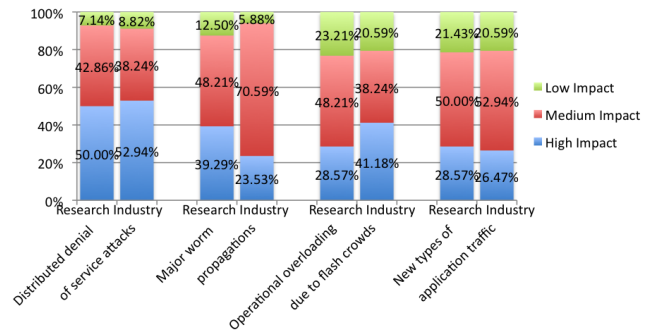
Possible inhibitors or fears that create difficulties for the acceptance of online/Internet services by the general public were also ranked according to job area. The weighted rank is presented in Table V, which includes the percentage of respondents that ranked each factor the most likely to be an inhibitor or fear<sup>5</sup>. Interesting differences in perceptions can be observed in these results as well. While *data leakage and privacy concerns (information disclosure)* is ranked first by respondents from Research as the most likely inhibitor (44.64%), it is ranked second in Industry (52.94% indicated it as the most likely inhibitor). Conversely, *misuse of personal data and impersonation (spoofing, repudiation, elevation of privileges)* is ranked first in Industry as the most likely inhibitor by 67.65% respondents, whereas it ranked second in Research (41.07% indicated it as the most likely inhibitor).

<sup>4</sup>Participants were allowed to rank more than one threat as #1, and for this reason the sum of percentages of threats ranked as the most likely exceeds 100%.

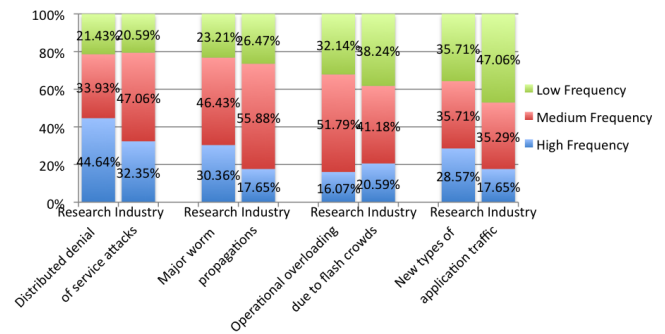
<sup>5</sup>Participants were allowed to rank more than one factor as #1, and for this reason the sum of percentages of factors ranked as the most likely exceeds 100%.

TABLE V  
WEIGHTED RANK OF MOST LIKELY INHIBITORS OR FEARS FOR THE  
ACCEPTANCE OF ONLINE/INTERNET SERVICES BY THE GENERAL PUBLIC  
ACCORDING TO JOB AREA

Rank		Description	% most likely	
Research	Industry		Research	Industry
#1	#2	Data leakage and privacy concerns (Information disclosure)	44.64%	52.94%
#2	#1	Misuse of personal data and impersonation (Spoofing, Repudiation, Elevation of privileges)	41.07%	67.65%
#3	#3	Lack of security and data integrity on the network (Tampering)	28.57%	29.41%
#4	#4	Unavailability of the services when they are needed (Denial of service)	17.86%	11.76%



(a) Impact of traffic issues on the operation of future networks

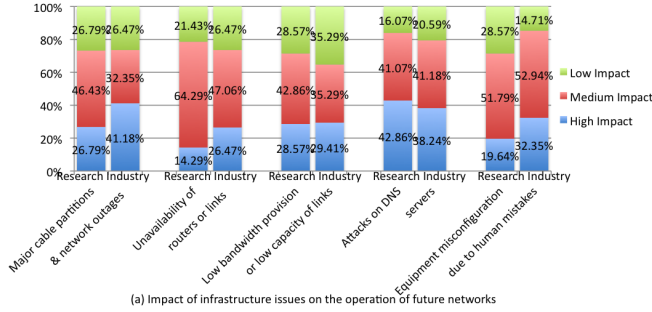


(b) Frequency of traffic issues on the operation of future networks

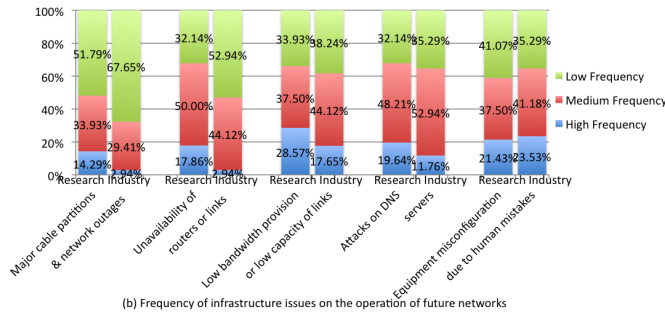
Fig. 8. Perceptions in terms of the impact and frequency of traffic issues on the operation of future networks according to job area

Fig. 8(a) and Fig. 8(b) show the perceptions of the respondents in terms of the impact and frequency of traffic issues in future networks, according to their job area. In terms of impact, it can be seen that *distributed denial of service attacks* and *new types of application traffic* are regarded very similarly by respondents from Research and Industry, with the former being considered as having the highest impact amongst all the traffic issues. However, the impact of *major worm propagations* and *operational overload due to flash crowds* is regarded differently by group of respondents, with the former

considered by Researchers as having a higher impact, and the latter considered by Industry experts as having a higher impact. In terms of frequency, *distributed denial of service attacks* is expected to occur more often by both groups of respondents. Among respondents from Research, *operational overload due to flash crowds* is expected to occur with the least frequency, whereas in Industry *new types of application traffic* is considered the least frequent traffic issue.



(a) Impact of infrastructure issues on the operation of future networks



(b) Frequency of infrastructure issues on the operation of future networks

Fig. 9. Perceptions in terms of the impact and frequency of infrastructure issues on the operation of future networks according to job area

Fig. 9(a) and Fig. 9(b) show the perceptions of the respondents in terms of the impact and frequency of infrastructure issues in future networks, according to their job area. It can be seen that *major cable partitions and network outages* are considered the issue with the highest impact by respondents from Industry (considered an issue of high impact by 41.18% respondents). Among respondents from Research, *attacks on DNS servers* are understood as having the highest impact (considered an issue of high impact by 42.86% respondents). In contrast, *unavailability of routers or links* was indicated as having the lowest impact by both groups: only 14.29% of respondents from Research and 26.47% of respondents from Industry considered it as having a high impact on the infrastructure. In terms of the frequency of these infrastructure issues, the profile of the responses given by respondents from both groups is very differing. For example, *major cable partitions and network outages* and *unavailability of routers and links* are perceived by respondents from Research as having a much higher impact compared to the understanding of Industry experts. Moreover, the issue with the highest frequency among respondents from Research is believed to

be *low bandwidth provision or low capacity of links* (28.57% indicated it as having a high frequency), whereas for Industry experts *equipment misconfiguration due to human mistakes* is believed to have the highest frequency (23.53% indicated it as having a high frequency).

TABLE VI  
WEIGHTED RANK OF MOST EFFECTIVE STRATEGIES IN THE EVALUATION OF RESILIENCE IN FUTURE NETWORKS ACCORDING TO JOB AREA

Rank		Description	% most effective	
Research	Industry		Research	Industry
#1	#1	Stress tests on real testbeds	48.21%	52.94%
#2	#2	Metrics and measurement analysis	46.43%	20.59%
#3	#4	Predictive data analysis	44.64%	11.76%
#4	#5	Simulation studies	30.36%	5.88%
#5	#3	Multi-layer data correlation and visualisation	25.00%	17.65%

Finally, we compared the responses from each group in terms of the most effective strategies in the evaluation of resilience in future networks. The rank is presented in Table VI, which includes the percentage of respondents that indicated a strategy as the most effective. Both groups regarded *stress tests on real testbeds* and *metrics and measurement analysis* as the two most effective strategies. However, their perceptions are very different with respect to the other strategies. Interestingly, *simulation studies* was indicated by 30.36% respondents from Research as the most effective strategy, but by only 5.88% respondents from Industry.

## VI. CONCLUDING REMARKS

The threat landscape on network operation is evolving. This is due to a combination of various new factors such as social and human factors (social engineering, new applications, and interpersonal trust), new types of devices, applications and end-systems (e.g. iPads, Facebook, e-Banking, iPlayer, etc.), as well as network and infrastructure vulnerabilities (e.g. network attacks, failures and misconfiguration). In order to understand the impact of emerging and future threats to network operations, we have asked a selected group of experts in the area of computer networks for their input. All the data presented in this report was obtained using an online questionnaire, which was answered by 160 experts in the subject. Through this questionnaire we were able to capture significant insights into how they perceive the causes, drivers and relevance of future threats to network infrastructures.

In this report, we presented our initial findings. We developed a cross-tabulated analysis comparing the perceptions from different groups of experts according to their job area (Research and Industry). We found a significant discrepancy between the priorities of Research and Industry. In particular, we observed that malicious network traffic attacks are the most likely threat according to experts from Research, whereas Industry experts perceive the exploitation of human factors as the biggest threat. In the same line, Research respondents consider data leakage as the most likely inhibitor of online services, whereas the misuse of personal data is the most likely

inhibitor for Industry experts. Where this discrepancy comes from is currently being investigated. One reason might be the increased usage and growing commercial importance of user-centric online services.

Perhaps more surprisingly, the study shows that physical attacks to communications network infrastructure are deemed low priority risk, and experts may be underestimating the threat to Internet security posed by these attacks. Less than 9% of Industry and Research experts who responded to the survey considered physical attacks to the infrastructure to be a likely threat to future Internet security. This contrasts with our increasing reliance on the digital economy, including online services provided by governments and businesses. We expect that the full set of results presented in this report can assist in the identification of priorities to be addressed within each context in order to build more secure and resilient networks and communication infrastructures.

This is an interim report based on data collected between November 23<sup>rd</sup> 2010 and April 5<sup>th</sup> 2011. It focuses on the comparison between the perceptions of Research and Industry with respect to emerging and future network threats. A full report with detailed analysis of the complete data set will be presented once the survey has been closed. Hence, as part of our future work, we are going to develop a similar analysis comparing the perceptions of respondents according to their country. We understand that different countries will have different needs in terms of support infrastructure and therefore different perceptions on the threats that will impact the future Internet. We will focus the analysis on the perceptions from British and Indian respondents because one of our aims is to identify areas of collaboration and synergy between UK and India, as well as to understand their specific needs.

The research team includes Lancaster University (led by Dr. Andreas Mauthe), University of Ulster (led by Professor Gerard Parr) and IIT Madras India (led by Professor Hema Murthy). The work falls under The India-UK Advanced Technology Centre (IU-ATC) in Next Generation Networks

Systems and Services which is funded by the UK Government through the Research Councils UK Digital Economy Programme and by the Indian Government's Department of Science and Technology (DST). The collaboration specifically deals with the development and exchange of knowledge and technology between India and UK but also with a collaboration between academia and industry in an increasingly more important market. Currently, the IU-ATC represents the largest India-UK collaboration of its kind between both countries.

## REFERENCES

- [1] H. Bos, E. Jonsson, S. Ioannidis, E. Kirde, and C. Kruegel, "Future threats to future trust," *Future of Trust in Computing Conference, Berlin, Germany*, July 2008.
- [2] *Digital Britain: Final Report*. Kew, Richmond, Surrey: Department for Culture, Media and Sport and Department for Business, Innovation and Skills, June 2009, ch. 7: Digital Security and Safety.
- [3] BBC News, "Internet-based attacks on critical systems rise," <http://www.bbc.co.uk/news/technology-13122339>, 19th April 2011.
- [4] G. Ollmann, "The opt-in botnet generation: Social networks, hacktivism and centrally-controlled protesting," Damballa, Tech. Rep., 2010.
- [5] I. Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian* May 17, 2007.
- [6] *The Guardian*, "Apple ipad blocked in israel," <http://www.guardian.co.uk/technology/2010/apr/16/apple-ipad-blocked-israel>, April 2010.
- [7] Trend Micro, "The future of threats and threat technologies: How the landscape is changing," Trend Micro, Incorporated, Tech. Rep., December 2009.
- [8] T. Thornburgh, "Social engineering: the "dark art"," in *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development*. New York, NY, USA: ACM, 2004, pp. 133–135.
- [9] J. Nagy and P. Pecho, "Social networks security," in *SECURWARE '09: Proceedings of the 2009 Third International Conference on Emerging Security Information, Systems and Technologies*. Washington, DC, USA: IEEE Computer Society, 2009, pp. 321–325.
- [10] R. Gibson, "Who's really in your top 8: network security in the age of social networking," in *SIGUCCS '07: Proceedings of the 35th annual ACM SIGUCCS conference on User services*. New York, NY, USA: ACM, 2007, pp. 131–134.
- [11] H. Bos, E. Jonsson, E. Djambazova, S. Ioannidis, K. Dimitrov, E. Kirde, and C. Kruegel, "Anticipating security threats to a future internet," *EU/FP7 FORWARD*, 2009.