The Risk of Relying on a Public Communications Infrastructure

Johannes de Haan

Network Manager Directorate
EUROCONTROL
Brussels, Belgium

Fabio Massacci, Pierantonia Sterlini

Dipartimento di Ingegneria e Scienza dell'Informazione
University of Trento
Trento, Italy

Peter Bernard Ladkin

Causalis Ingenieurgesellschaft mbH.
Bielefeld, Germany

Christian Raspotnig

AVINOR ANS
Oslo, Norway

Abstract Air Navigation Service Providers (ANSPs), and other critical service providers, are gradually replacing dedicated analogue and Digital Communications Infrastructures (DCI) by a public DCI, provided by a limited number of service providers. This cost-driven measure clashes with the need to assure the safety of ANSPs' operations by providing safety cases in which they show what has been done to reduce the risk to an acceptable level. In case of DCI, however, they are not always able to prove this because modern DCI are very complex, subject to dynamic (re)configuration, and several level of subcontracting. Traditional risk analysis processes are not equipped for this kind of dynamic assessment. Furthermore, the information provided by the communications service providers is—in general—not sufficient for such assurance purposes. Being public, DCI are also subject to security attacks that would not have been physically possible in the past with dedicated DCI. In this paper, we highlight risks that do not appear in typical risk analyses. We discuss general and air-traffic-management-specific challenges in using outsourced communication services. We conclude with some technical, organizational and potentially regulatory steps, which we believe are needed to improve the transparency and long-term safety and security of this increasingly complex infrastructure. We also provide some insight on future challenges by summarising interviews with key stakeholders.

1 Introduction

Modern society increasingly depends on a functioning public *Digital Communications Infrastructure (DCI)*. Not only the “visible” part of the Internet, but also parts that are invisible to the general public, such as communication links between ATC centres in different countries, play an essential role in the overall functioning of modern society. In the past, ANSP corporate communication took place over separated and dedicated (Digital[1]) Communications Infrastructures. Requirements in terms of performance, security and overall resilience for DCI were often directly contracted between the service provider and the organisation.

In the past, the physical connections were under the vertical managerial control of one provider. Now, the connections are virtualised, have a much deeper layering of protocols, and lay under the control of multiple providers. The analysis of resilience properties has become so complex that third party verification is barely practical, if it can be accomplished at all (Noam, 1987).

This situation is aggravated through concentrating previously diverse ANSP services (Figure 1) on the same infrastructure (Figure 2), because in many cases there are no other options. There is—as yet—no clear regulatory framework to ensure the availability of the infrastructure, nor demanding mitigation actions from the entities using this infrastructure. Such regulation may allow, for example, a realistic evaluation of the pathways by which Denial of Service (DoS) could be achieved, and thus enable regulators and providers to engage in prophylactic measures. It seems to us that the risk associated with the use of the digital communications infrastructure (DCI) has been underestimated.

[1] Voice communications is still analog in many ANSPs and is slowly moving to VoIP.

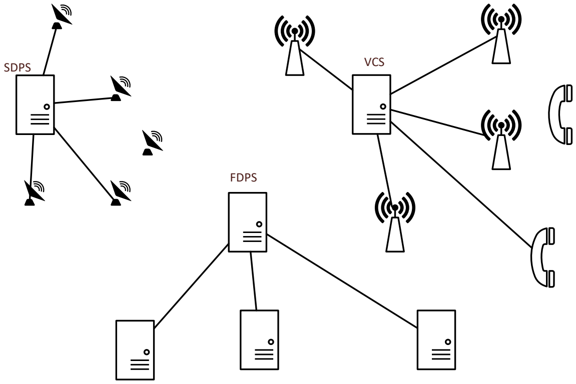

Figure 1: "Old" distributed architecture

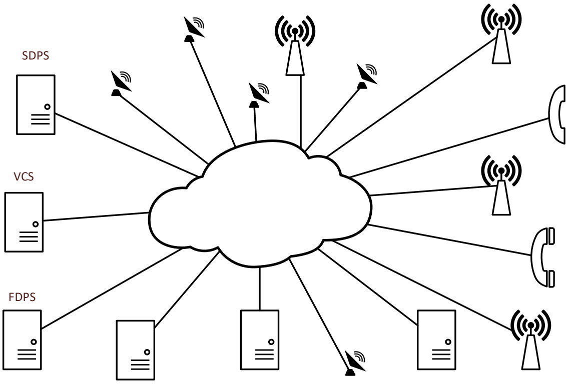

Figure 2 "New" concentrated architecture

2 General challenges

The main challenge in assessing (and assuring) the resilience of the DCI is the lack of transparency of this infrastructure. This lack arises through:

- Inherent complexity of the infrastructure (both static and dynamic)
- Fast growth of the infrastructure
- Many providers across the organisational network Tiers[2]

Currently, providers can realistically claim that they are not able to provide verifiable information on the (dynamic) state of their infrastructure to third parties. However, without such information, Critical Infrastructure Providers (CIPs) relying on a DCI are not able adequately to assess the risk associated with its use.

[2] The Internet infrastructure is organised in three tiers. Tier 1 comprises the large international network connections, Tier 2 are the national high bandwidth networks and Tier 3 are the single homed service providers.

An example of increased risk through lack of transparency is that CIPs relying on a DCI are not always informed of the occurrence of maintenance activities. This does not inevitably affect immediate service provision, but it reduces the redundancy in the network. In normal ANSP practice, redundancy is an important resiliency property, and reduced redundancy is accompanied by a reduction of traffic in the affected sectors. If the loss of redundancy is not known, traffic will not be reduced and the operational safety case may be violated.

Telecommunications provision is currently aimed at a mass market and this makes it difficult for small niche customers such as ANSPs to assure that their requirements are met. The ultimate cost of fulfilling these requirements inclines towards the prohibitive (Air Traffic Management and other transport sectors are comparatively relatively small customers). Meeting the requirements of niche critical-infrastructure providers such as ANSPs could theoretically be assured through regulating DCI, but such regulation would not necessarily reduce the involved costs, which someone would have to pay.

Another challenge is to assess the risk generated by concentrating service onto few technological systems when this is combined with the sharing of the same services by several providers. This is cost effective when everything works well. However, concentration of the different services and their sharing creates (at least) two types of risk:

- **Shared Vulnerability Failure Mode** (SVFM): The inadvertent or intentional exploit of a single vulnerability of a single (off-the-shelf or bespoke) component type can become a large-scale outage when the components of this type are used in several parts of the DCI (common cause failures).
- **Collateral Cyber Attack Failure Mode** (CCAFM): Some aggressors might attempt to attack a shared DCI and take it down for purposes unrelated to that part of the DCI, which is used for servicing a critical infrastructure.

As one example of severe collateral damage, the French telecom provider OVH was hit by a Distributed Denial of Service (DDoS) attack a hundred times larger than most of its kind in September 2016. Another example: in October 2016, the internet slowed or stopped for nearly the entire eastern United States, as the tech company DYN, a DNS provider, came under another major DDoS assault. Initially, this was speculated to be a nation-state scaling up an effort to influence the US election. However, the indictment by the FBI of three individual hackers with no connection to nation-states or criminal organizations shows that the shutdown was the effect of a turf war between booter service providers for Minecraft computer game servers. Booter services (Hutchings & Clayton, 2016) are DDoS defenses (respectively attacks) offered by groups of hackers to on-line multiplayer gamers to protect one's game server (respectively disrupt other players' servers).

The reliance on Commercial Off-The-Shelf (COTS) products in mission critical components is increasing the cost efficiency and—in general—the reliability of systems (because of “proven in use” technology), but it also increases the risk of SVFM events. An example is the Broadcom bug (Artenstein, 2017) which created a vulnerability in Apple and Samsung products, which relied on the dependable operation of this component. Despite the fact that the integrators (Apple and Samsung) put considerable effort into securing their systems, their reliance on a COTS component showed that such reliance on COTS dependability can be misplaced. The Spectre (Kocher, et al., 2018) and Meltdown (Lipp, et al., 2018) vulnerabilities provide further examples of this phenomenon.

A potentially unexpected source of additional issues is the web of DCI service providers. DCIs (especially high-bandwidth national and international links) are operated by a limited number of commercial providers (e.g. Deutsche Telekom, Orange). When domain-specific service providers such as SITA and Airinc in air transport or ANSPs use these DCIs, provision of services is based on standard Service Level Agreements (SLAs), defining amongst other attributes availability, response, and repair times up to physically-separated end–to–end routing.

Resilience of the DCI services has to be provided by the CPIs, for example through the use of different service providers between each communication-partner pair, and the use of technology to autonomously detect link outages and to switch to alternative circuits in case of a link failure.

A common problem with such resilience measures is that they are based on assumptions which are very difficult to verify on the web of sourcing providers. An example is the requirement for physically separated end–to–end routing. It is not possible to trace the physical route exactly for CPIs using a DCI. Even for the service provider itself this may be very difficult.

- **Shared Subcontracting Failure Mode** (SSFM): The communication channels necessary for recovery in case of a service degradation or failure may well be unavailable during such a failure, since they might use the exact same infrastructure at a lower layer. An ANSP might contract two different providers for resilience (for example a mobile and a fibre telecom provider). However, except for the first link they might be actually using the very same backbone of a third provider, as such agreements are increasingly common (Meddour, Rasheed, and Gourhant 2011)

We suggest it is likely that this kind of problem will become more common in Air Traffic Management (ATM).

3 ATM specific challenges

ATM is a distributed socio–technical system, which is critically dependent on available communications amongst system participants.

Table 1: Communication types and related failure scenarios[3]

Type of communications	Severity of a failure
Air-ground requests and instructions	Failure of air-ground communications directly affects the ability to maintain separation between aircraft and leads to airspace closure.
Ground-ground coordination	Failure of ground-ground communications affects the ability to coordinate participating flights between ATC centres and leads to possibly-severe traffic restrictions.
Surveillance data	Loss of surveillance data may lead directly to loss of separation and certainly leads to airspace closure.
Flightplan data	Loss of flightplan data significantly reduces ANSP ability to service air traffic.

Note that risk in safety-related contexts is usually taken as a combination of the likelihood that an event will happen combined with the (usually worst-case) severity of the event. When considering potential new failure modes, assessing likelihood is not necessarily feasible in a cyber-security case; cyber-security likelihoods are not static, but are dependent on potentially rapidly changing contextual parameters such as:

- Recognition and understanding of vulnerabilities by operators and potential exploiters;
- The existence/development of exploits;
- The motivation and opportunity of an aggressor to execute an exploit.

For example, recent approaches that try to estimate the likelihood of attacks based on the data of IT infrastructure includes among the parameters of analysis the power of the attacker (Allodi and Massacci, 2017). Hence, the likelihood can only be determined for a given attacker. Thus, we list in Table 1 the severity of a given failure without estimate of likelihood.

Many instances of these “failure modes” are already recognised by ANSPs as critical. For this reason, diverse communications kit suppliers may be used, in order to attempt to assure physical independence of systems and thereby reduce the chances of common-cause failure. However, communications are carried over infrastructure provided by third-party service providers, whose contractual arrangements can lead to nominally independent systems being implemented on the same physical infrastructure (Spriggs, n.d.) (Artenstein, 2017). Also, failure analysis and common-cause failure analysis is presaged on accidental failures. An intentional attack on communications infrastructure is not necessarily thwarted simply through physical independence. There is the possibility of a wide-scope communications failure, by which we mean that many nominally-independent

[3] It should be noted that in case of a wide scope communications failure scenario multiple or even all communication type may become unavailable.

communications systems effectively-simultaneously fail. This can occur for example through the failure modes we have described above.

ANSP systems are predicated on the principle of resilience through graceful degradation; that when certain functions fail, other functions remain available to provide critical functionality “down to” a minimal operational system in order to reach a safe state. The minimal operational system is traditionally voice communication between participating aircraft and ATCO[4].

Some pertinent observations:

- The information transmitted over the system is standardized (standard clearance procedures);
- The channel itself can be degraded (e.g. poor radio transmission/reception; sporadic availability);
- Degradation can be mitigated by using multiple channels (e.g., UHF, microwave; VHF radio).

It is nevertheless physically possible for this system to fail overall. There are (at least) four ways in which it may fail:

- A wide-area electromagnetic disturbance inhibiting the minimal-necessary communication (e.g., a major space weather event);
- A sustained attack on the ground-based infrastructure (say, a DDoS attack);
- A partial degradation in the case in which air-traffic density is too high to allow graceful service degradation without compromising safety (the risk of collision is strongly raised in some part of the system);
- A severe degradation of the IP backbone by other than an attack (say a result of misconfiguration, or a SW problem in network kit, much of which comes from one supplier) which then “avalanches”.

The ATM system has demonstrated that it is able to cope with local failures and failures that only affect parts of the DCI. Thus far, no wide-scope DCI failures have been observed in operational environments.

A preview of the potential damage of a major communications outage arose during the Belgocontrol power outage incident on 27 May 2015. During this event, almost all equipment at the Belgian ATC centre in Steenokkerzeel was left without power, which completely incapacitated Belgocontrol’s ATCOs. Under such circumstances, the traffic in the Belgian airspace would normally be handed over to adjacent centres. Unfortunately, all communication lines were taken down as well, so the hand over was not possible using the “normal” channels. The supervisors managed to contact the adjacent centres using their mobile phones. In case of a wide-scope failure of the DCI, it is very likely that the mobile phones would also not have been available, because the mobile phone network also uses the major communications backbones.

The consequences of a wide-scope communications failure, therefore, would be a major disruption of European air traffic at best, potentially culminating in a catastrophic scenario where the residual ATM capabilities are insufficient to get all

[4] Air Traffic COntroller

aircraft on the ground safely. Such a failure will thus be most likely more severe than the consequences of a major power failure. There are several reasons for this:

1. In contrast to fall-back systems for a power failure, which can be local, communications back-up channels need to be present on both ends of the communication.
2. All current ANSP operational contingency plans are based on the assumption that some communication capabilities remain available.
3. With a large-scale communications failure, the ability to coordinate for a quick recovery also disappears.

This all makes wide-scope communications failure a qualitatively different failure mode from those communications failures that are currently mitigated within ANSPs.

4 Supporting interviews

The concerns which we have raised in previous sections turn out to be shared, or at least hinted at, by diverse ATM professionals. Some of the authors organised several meetings with over 60 stakeholders, on different emerging threats to ATM (from security, to trade-off between organizational measures and technical measures, as well as fairness of regulatory intervention) as well to other critical infrastructure. Various techniques exist for knowledge elicitation (Hoffman et al. 1995), but a variant of structured or semi-structured interviews are most commonly involved in task analysis (Spector et al. 2014, Ch. 42). For 19 stakeholders who agreed to be formally interviewed, we conducted 30-40-minute in-depth semi-structured interviews which were recorded with participants' permission and transcribed into anonymous form. The aim of these semi-structured interviews was to discuss the main issues related to the emerging threats in the ATM domain, and the effectiveness of regulation to mitigate these upcoming risks. Not all interactions could be transcribed for security reasons (as in some cases the stakeholders illustrated specific, still active, vulnerabilities of the infrastructure under their purview). Interviews can be particularly useful to provide a qualitative validation of a formal model describing the impact of regulations or contractual arrangements (de Gramatica et al. 2017).

We illustrate these finding by the own words of some stakeholders representative of the different roles in the area and summarized in Table 2, interviewed in Nov-Dec 2014, arose through a purposive sampling (Halaweh 2012) method to represent a variety of roles specifically involved in the regulatory aspects of emerging threats in the aviation domain.

Table 2: Participants interviews

ID	Role	Organization
1	Head of ATM Security Unit	European Authority for Air Navigation
2	EU Aviation Regulator	EU Directorate for Transport
3	Responsible of Security Training programs	IATA
4	Office for National Security	European National Government
5	Security Manager and Training Instructor	Airport and Civil Aviation Authority
6	Security Manager	Airport

At first they agree on the issue of connectivity being a major issue and that this is progressively impacting also the providers of critical infrastructure such as ATM:

> “we are much more dependent on the internet now, but at the same time this causes the greatest threat. Our critical infrastructure is dependent on the internet as well, not just citizens.” [#4]

This is well recognized also by one of the regulators [#2] who also stresses the strong economic push for such changes, who were confirmed also by other interviewees [#3]. They both used airports to illustrate the scale and the strength of the economic drivers:

> “You have approximately 660 airports in the EU. Of them, probably ten are very innovative and try to look at things differently, investing in new technologies, new processes and play with things to improve security and processes. Many airports tend to invest their scarce resources where they can get the best return.” [#2]
> “Airports tend not to invest more than what is necessary, this is natural because they run a business in a good financial way.” [#3]

The need to address the cybersecurity challenges of technical transformation is well summarized by one of the interviewees:

> “The issue is that we already envisage a fast and quick change in a lot of processes, like the Air Traffic Management and we have to adapt very quickly to respond to the new threat scenarios. This is becoming more and more challenging. I am not sure that we will be able with the current regulatory framework […] to move at the same pace than the threats” [#1]

The need to modify regulation is also recognized by other actors, so that we might not have a uniform regulation that applies unconditionally to everything, but rather one that is able to discriminate between different types of risk areas:

> “There should be a unified regulation, but there should be also a risk-based approach. If there is a high risk, there should be some plug-ins to the normal baseline regulation.” [#3]

This may require more than regulation, namely also the technical possibility to manage risk as we have advocated, by making third party risk verification possible:

> “In formulating regulation we have to identify the risks and what we can do about them and then we draft the regulation. There may be also some risks where we cannot do anything about, for example, they may be too difficult to mitigate without hindering the flow of traffic. Where it is unfeasible to implement a mitigation, risk is managed” [#2]

It might be a simple conclusion that the concerns that we raise are only applicable to ANSPs which the broader DCI industry could see as a very limited and niche application. Hence, regulators might be actually unwilling to pursue broad changes that might significantly affect the economic viability of DCI operators (Clifton, Comin, Díaz-Fuentes, 2011).

To make sure that this was not the case we also carried a confirmatory interview on another critical infrastructure. The focus on power supply seems particularly relevant since Belgocontrol power outage incident mentioned above. The chair of the technical committee of the networks of energy transmissions operator was therefore interviewed.

At first we obtained confirmation that the energy sector face the same challenges of ATM second in terms of increasing reliance on the public DCI:

> “Another thing is connectivity: every company wants more and more data and they are connected to more and more company systems. They are opening more doors than they are closing.”

The process of dependence on the DCI is arrived at a point where there is no operation without a DCI. Whilst this was essentially obvious from an ANSP perspective, this now show that the impact of DCIs is now ubiquitous to be no longer a characteristic of the niche ATM market:

> “you can no longer run the electricity networks effectively without IT in Europe…. Ten years ago, this was not an issue: you could have operated the transmission network manually. Nowadays we do not have a manual procedure that can effectively manage the network. It is too complicated.

The possibility of collateral damage that we have identified as Shared Vulnerability Failure Mode and Collateral Vulnerability Failure Mode and we have illustrated in Section 2 with the DYN example is also broadly accepted in this domain:

> “Even if [malware/virus] is not targeting the energy sector, they could take out the energy sector because the vulnerabilities they exploit are not sector specific.”

5 Conclusion and discussion

In many ANSPs, the DCI is treated as a commodity that can be obtained from the market. Its assurance relies on SLAs, which are often limited to the standard provisions offered by the provider. The DCI providers are operating and maintaining their infrastructures for the mass market. ANSPs are relatively small customers with relatively stringent and costly requirements, which do not fit well with the business model of the provider for the mass market.

The standard conditions in current SLAs are not in line with the criticality of the DCIs for ANSP operations. Even if additional requirements and constraints are included in the SLAs, there is hardly any possibility to verify continued compliance. ATM is used as a prime example in this paper, but it is by no means the only domain affected (see the comments from interviewee #4). This situation can affect society much more widely.

It follows that a number of steps need to be taken to secure the dependability and resilience of the DCI in a wider context:

- **From the perspective of Critical Infrastructure Providers relying on a DCI:** Create policies and procedures that explicitly address the criticality of the DCI (an SLA is unlikely to be sufficient) and include the DCI in safety and security assessments. ANSPs must develop procedures to handle traffic when the communications with adjacent centres are limited. For example, they could consider the use of terrestrial independent satellite communications (e.g., Iridium) for emergency situations (we note, though, that satellite communications are also vulnerable to a Carrington Event);
- **From a technical perspective:** Develop better mechanisms for dynamic third-party verification of data-flow characteristics of the networks, including the possibility to provide this information on-line directly to organizations that rely on the DCI for critical services;
- **From the political perspective:** Consider the DCI as amongst other things *providing critical infrastructure services*; creating regulations and oversight that is in line with the criticality of this part of the DCI (as in the case of electrical power supply). This is not currently foreseen in EC2016/1148 Annex II (European Commission, 2016).

The reviewers of earlier versions of this document had some comments that we would like to share for further discussion.

Comment: *Many mission-critical industries and sectors rely on the commercial model using SLAs and associated instruments. This seems to work fine (with an occasional outage). They tend to rely on large amounts of redundancy. Is air traffic management really so different from say, healthcare or banking?*

Reply: We have not seen a wide-scope communications failure of the sort we are considering in this paper in any of the industries mentioned. We suggest that a wide-scope failure would also cause significant problems in healthcare and banking. But these are not our subject here. These large sociotechnical systems, as systems, are more complex and less monolithic than air traffic management. We could surmise, for example, that a wide-scope communications failure in banking systems would disable the daily dynamic reconciliation of reserve requirements around the globe which is essential for the functioning of the entire banking sector, which might well lead to an emergency and a financial crash. But all that is for another paper similar to this on the banking sector.

In air traffic management and control, an SLA would not be worth the paper it is printed on when an accident results from a wide-scope communications outage.

Comment: *It seems a good idea to include the DCI in safety and security assessments but the commercial communications provider may not oblige.*

Reply: Yes. That is why there may have to be regulation. We suggest the chance of such regulation is quite good, when the risks of wide-scope communications failure for various critical infrastructure are investigated: most depend on the communications networks which are not themselves yet seen as critical.

Comment: *What about ground-based systems in the event of a Carrington Event?*

Reply: In fact, the majority of communications is effected via ground based networks. Satellite-based communication is only used where no ground alternative is available, e.g. for oceanic traffic[5].

Comment: *It might be possible to consider a combination of network providers and failover technologies (satellite, microwave) together to provide, as a whole, the overall critical communications infrastructure and to protect it accordingly.*

Reply: Regulation would be required to accomplish this. In any case, designated critical or not, such a combination is still vulnerable to misconfiguration of critical network elements, cyber-attacks or a large space weather events (Carrington Event). We believe the possibility of wide-scope communications outages has been generally underestimated. We have attempted to address the issue here just for one sector.

6 Acknowledgements

Part of the work behind this paper has been supported by the European Union’s 7th Framework Programme under grant agreement 285223 (SECONOMICS) and the Horizon H2020 FP under grant agreement 675320 (NeCS). We thank the Eurocontrol Task Force on the Resilience of Digital Communications Infrastructure (RDCI) for detailed commentary (some of the authors are members of RDCI).

[5] According to space-meteorologists, a major space weather event like the 1859 Carrington Event is capable of taking out any electrical system and maybe all of them.

7 References

[1] Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis, 37*(8), 1606-1627.

[2] Artenstein, N. (2017). *BROADPWN: REMOTELY COMPROMISING ANDROID AND IOS VIA A BUG IN THE BROADCOM WI-FI CHIPSET.* Exodusintel. Retrieved from https://www.blackhat.com/docs/us-17/thursday/us-17-Artenstein-Broadpwn-Remotely-Compromising-Android-And-iOS-Via-A-Bug-In-Broadcoms-Wifi-Chipsets-wp.pdf

[3] Clifton, J., Comin, F., & Díaz-Fuentes, D. (2011). From national monopoly to multinational corporation: How regulation shaped the road towards telecommunications internationalisation. *Business History, 53*(5), 761-781.

[4] de Gramatica, M., Massacci, F., Shim, W., Turhan, U., & Williams, J. (2017). Agency Problems and Airport Security: Quantitative and Qualitative Evidence on the Impact of Security Training. *Risk Analysis, 37*(2), 372-395.

[5] European Commission. (2016, July 06). *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Retrieved from eur-lex.europa.eu: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[6] Halaweh, M. (2012). Using grounded theory as a method for system requirements analysis. *Journal of Information Systems and Technology Management*, 23-38.

[7] Hoffman, R., Shadbolt, N., Burton, M., & G, K. (1995). Eliciting knowledgefrom experts: A methodological analysis. *Organizational Behavior and Human Decision Processes*, 129-158.

[8] Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior, 37*(10), 1163-1178.

[9] Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., . . . Yarom, Y. (2018). *Spectre Attacks: Exploring Speculative Execution.* Retrieved from ArXiv.org: https://arxiv.org/pdf/1801.01203.pdf

[10] Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, Werner, . . . Hamburg, M. (2018). *Meltdown.* Retrieved from arXiv.org: https://arxiv.org/abs/1801.01207

[11] Maxwell, J. (2009). Designing a qualitative study. In L. Bockman, & D. Rog (Eds.), *The SAGE Handbook of Applied Social Research Methods* (pp. 69-100). SAGE Publications.

[12] Meddour, D. E., Rasheed, T., & Gourhant, Y. (2011). On the role of infrastructure sharing for mobile network operators in emerging markets. *Computer Networks, 55*(7), 1576-1591.

[13] Noam, E. M. (1987). The public telecommunications network: a concept in transition. *Journal of Communication, 37*(1), 30-48.

[14] Schintler, L. A., Gorman, S. P., Reggiani, A., Patuelli, R., Gillespie, A., Nijkamp, P., & Rutherford, J. (2005, December). The public telecommunications network: a concept in transition. *Networks and Spatial Economics, 5*(4), 351–370.

[15] Spector, M. J., Merrill, D. M., Elen, J., & Bishop, M. J. (2014). *Handbook of Research on Educational Communication and Technology.* New York, NY: Springer.

[16] Spriggs, J. (n.d.). *Assurance by Proxy.* Retrieved from scsc.org.uk: http://scsc.org.uk/file/378/20—John-Spriggs—Assurance-by-Proxy.pdf

[17] Ugur, M. (2009). Regulatory quality and performance in EU network industries: evidence on telecommunications, gas and electricity. *Journal of Public Policy, 29*(3), 347-370.

[18] US Department of Justice, Office of Public Affairs. "Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant DDoS Attacks. Defendants Responsible for Creating “Mirai” and Clickfraud Botnets, Infecting Hundreds of Thousands of IoT Devices with Malicious Software". Dec. 2017. Available on the internet at https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving

[19] Wu, I. (2004). Canada, South Korea, Netherlands and Sweden: regulatory implications of the convergence of telecommunications, broadcasting and Internet services,. *Telecommunications Policy,* 79-96.