This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No.: 607480

LARGE SCALE INFORMATION EXPLOITATION OF FORENSIC DATA

From Risk Management to Security Culture: the Changing Organization of Security

LASIE Project

FP7 – SEC-2013.1.6-1 – Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes – Integration Project

Grant Agreement n°: 607480

Start date of project: 1 May 2014

Duration: 42 months

Document ref.: n/a

Peace Research Institute Oslo (PRIO)

Oslo, 13 June 2017

From Risk Management to Security Culture: the Changing Organization of Security

A breakfast seminar by and with Dr Mark B. Salter[1]

A public report by Ida Rødningen (PRIO)

Introduction

On 13 June 2017, Dr Mark B. Salter held a public breakfast seminar at the Peace Research Institute Oslo (PRIO). With the title "From Risk Management to Security Culture: The Changing Organization of Security", the seminar was initiated by the research team from the LASIE project[2] at PRIO, and organized within the framework of the project. LASIE, or 'Large Scale Information Exploitation of Forensic Data' (2014-2017), is a European Union (EU) co-founded research project conducted under the 7th Framework Programme for Research and Development (FP7). The aim of the 3,5-year project is to design, adapt and implement an open and expandable framework that will significantly increase the efficiency of current forensic investigation practices, by providing an automated initial analysis of the vast amounts of heterogeneous forensic data that analysts have to cope with. The end result of LASIE will be a new smart surveillance tool, which integrates different surveillance methods. It will be able to assist end-users in extracting information from a variety of data, for instance Close-Circuit Television (CCTV) databases, audio recordings, scripture and handwriting and multiple-format biometric information. The ultimate goal is for the LASIE "gadget" to be able to provide end-users (police, etc.) with more sophisticated evidence in the aftermath of a crime.

The research consortium consists of 18 technical and non-technical partners from all over Europe, and PRIO, as a partner in the project, is responsible for an ethical and societally acceptable development of the "gadget". This includes legal as well as ethical considerations, and covers potential issues relating to privacy and personal data protection. Partly, PRIO's responsibility is to continuously monitor and report back to the consortium via deliverables on emerging societal challenges, such as public acceptability and relevant legal developments. In addition to monitoring the project to ensure that its outputs are ethically sound and compliant to relevant legal regulations, PRIO advices on how to make sure that the forensic evidence compiled by the LASIE framework will be admissible by courts of law in Europe.

[1] Mark B. Salter is a professor at the School of Political Studies, University of Ottawa. He was the 2014 Canadian Political Association Teaching Excellence Prize winner. In 2007, he was the recipient of the National Capital Educator's Award and the Excellence in Education Prize at the University of Ottawa. In autumn 2008, he was Visiting Fellow at the Centre for Research in the Arts, Social Sciences, and Humanities, Wolfson College, and Visiting Scholar at the Centre of International Studies at the University of Cambridge. He is editor of "Making Things International 1" and "Making Things International 2", "Research Methods in Critical Security Studies", "Politics at the Airport", as well as special issues on "Border Security as Practice", "Critical Security Studies in Canada" and the Forums of International Political Sociology. Salter is also editor of the journal *Security Dialogue*.

[2] Cf. www.lasie-project.eu.

Background to LASIE seminars at PRIO

Since 2016, PRIO – as a partner in LASIE – has organized four short seminars at its premises in Oslo, Norway to discuss with invited experts the most pressing societal issues arising from the LASIE research project. The adopted formula of such seminars involves an introduction to a given topic by chairperson (15 min.), a keynote by the invited expert (45 min.), up to two interventions from invited commentators (10 min. each), the response from the invited expert (10 min.) and, eventually, the discussion with the audience (30 min.) The seminars are organised either during a breakfast or a lunch and last two hours. Each seminar is followed by a public report such as the present one.

The first seminar hosted Dr Roger Clarke (Australian National University and the University of New South Wales) on 29 August 2016 and analysed the notion of "security".[3] The second seminar hosted Dr Mireille Hildebrandt (Vrije Universiteit Brussel) on 18 November 2016, examining the concept of artificial police agents.[4] The third and penultimate seminar hosted Dr Gemma Galdon Clavell (Eticas Research & Consulting; Universitat de Barcelona) on 17 February 2017, who gave a keynote presentation about the challenges facing smart cities and their development.[5] The current report thus synthesises the fourth and final seminar in the series.

This seminar was advertised internally within the LASIE consortium, as well as on PRIO's websites and in social media with the following description:

> *Aviation security has changed radically over the past twenty years with new threats and new technologies reshaping the airport and the travel experience. The way that body scanners have been adopted, regulated, and adapted illustrates how security, privacy and law are affected by governmental structures, market forces, and broader societal attitudes. In particular, the dynamics of the international aviation security regime condition the possibility of security and affect how technologies are integrated into a loose global system. The* millimeter *wave scanner failed to gain public acceptance in the United States and Canada, whereas the European Union was able to regulate that technology and craft public acceptance much more deftly. The integration of security and technology will then be connected to different public management approaches to risk management and security cultures.*

The seminar was attended by a large group of the LASIE consortium partners.

The views expressed in the following are solely those of the speakers, as communicated in the seminars, and do not reflect the views of the LASIE consortium as a whole, its individual partners nor the European Commission.

Opening of the seminar

The seminar was opened by PRIO's Stine Bergersen, a researcher and member of the PRIO's LASIE team. Bergersen welcomed the keynote speaker, discussants and audience, with an especial welcome to the members of the LASIE consortium, and proceeded to introduce the hosting institution, the LASIE project itself and PRIO's role as a project partner.

[3] Cf. http://www.lasie-project.eu/wp-content/uploads/2015/05/LASIE_Clarke_seminar_FINAL_ok_cleanv2.pdf.
[4] Cf. https://www.prio.org/utility/DownloadFile.ashx?id=323&type=publicationfile.
[5] Report still in the making.

The topic of the seminar was aviation security, and what seems to be a shift of directions in that context: a shift from risk management to an entire culture of security. The experience of travelling by plane has indeed changed in the last 20 years. As Salter writes himself in *Politics at the Airport* (2008): "Airports are vital and vulnerable nodes in the global mobility regime. The coordinated exploitation of security gaps on 9/11 and direct attacks on Glasgow, Madrid and other airport subsequently demonstrated that the lure of adventure and exotic destinations have been overlaid by anxiety, frustration and fear."[6]

The floor was given to Salter for his presentation.

Photo by Martin Tegnander, PRIO

Presentation by Dr Mark B. Salter, "From Risk Management to Security Culture: the Changing Organization of Security"

Salter started out presenting some basic assumptions about security he believes are shared by many: security and the perception of security is a) not the same thing, and b) socially constructed. There is not an objective condition of security that we can identify, but rather it is something fluid that is created. It is created in a dialogue between the public and the experts, but it's also mediated by technology, by the architecture and structure of those spaces in which we feel secure or insecure. Salter underlined that the focus of the seminar on the millimeter wave scanner, even though the airport security system is focused on detection at that one point, is to draw some relevant lessons for the

[6] Salter, Mark B (Ed.) *Politics at the Airport*, University of Minnesota Press, Minneapolis, 2008.

LASIE gadget in terms of the interpretation and presentation of the technology, and the way that it becomes publicly accepted.

Crucial in airport security is to make a balance between sterile and non-sterile environments at this moment of the screening point. The old magnetometer was introduced in 1972, and the metal detection archway had been the standard for over 20 years when the millimeter wave scanner was developed. Public perception of security had been based on and through this version of technology that they could see, and what they were familiar with. When the millimeter wave scanner was introduced in the mid-2000s, it produced very vivid images of naked bodies, rather than a benign "ding" if you had left your belt on. This caused an enormous amount of public pushback, and the sense of the invasion of privacy was substantial and unwarranted. This results in an interesting dilemma: the millimeter wave scanner is a better technology for the detection of threats against aviation security, yet the public appetite for it was close to zero. People thought it was dodgy, they were worried about naked images of their children.

Salter presented the audience with the first version of pictures from the millimeter wave scanner that the screening officers saw on the screen. After the pushback, in 2013 the ATR, or the Automatic Threat Detection system, was created. This system algorithmically extrapolated from the naked image to a "ginger-bread person" that gave you an "OK" or a "no-OK" sound. One of the reasons they did this was to protect privacy. In this transformation process, they also removed all capacity for memory in the machine itself. "One of the ways we are going to protect your privacy by design is taking out all the memory." In consequence, there is no way to know whether or not the machine made a good choice. This privacy-by-design solution means that the system is un-examinable – you can't tell how good it is. There is no case of significant detection at that screening point, but there is no data that it has failed either. This creates a fundamental tension between privacy-by-design design and the capacity to provide security, as well as the perception of security. Even though the ginger-bread man looks more benign, it nonetheless has a boy and a girl button. This can be problematic, because trans- and cross-dressed people are almost routinely sent off for secondary screening. That also the case for people with prosthetic limbs etc., so even though it removes one set of prejudices from the system it embeds another set.

After 9/11, the international aviation security regime and international organisations felt that they needed to reorient their security culture. The public management tool that they adopted was risk management. Part of the problem with risk management in this particular situation, Salter held, is the complexity of the system. It is unclear who is in charge of what, which are the different authorities, etc. Even if each of the different agencies did their own risk management, none of them would have an overall view of what the entire system looked like. Furthermore, part of the problem can also be found at the juncture between real risk and perceived risk. For example: being involved in a terrorist attack or plane crash are extremely rare instances but are perceived to be common, whereas suffering a heart attack is much more likely yet perceived very rare.

Salter argued that within this risk management complex there are two problems. Firstly, risk management is a way of schematizing the threat to a particular agency. One gauges the frequency, or probability, of attacks with their impact. Once these are ranked in a particular system, you essentially make four judgements. You either accept the risk (as part of doing business), mitigate the risk (by trying to reduce the probability of attacks), transfer the risk (by e.g. taking out insurance) or avoid the risk (by saying this is no longer our problem). The millimeter wave scanner was an attempt to mitigate the risk of attacks using explosives hidden in clothing.

Briefly going through the history of the millimeter wave scanner, Salter informed that Schiphol Airport was the first to adopt the machine. Canada has seen itself to be at the forefront of aviation security, both because of the Air India bombing in 1985 and because of the way the country reacted after 9/11. By 2010, 56 scanners were in use in Canada, followed by a huge public outrage. In 2013, the ATR software was introduced.

The public outrage around the machine was based on privacy concerns. The argument was that the scanner should not be able to show naked images of children, because that would amount to child pornography. The implication seemed to be that either you went through the scanner, or you went through a full-body cavity search. Part of the problem, Salter stressed, in terms of risk management, was that studies had showed that random selection of individuals was as effective as targeted selection. As mentioned earlier, there is a disjuncture between a technology that works better on the one hand, and public perception of the cost involved (in terms of privacy) and the security provided on the other. The expert opinion was not much better: there was no forensic data indicating that this had ever successfully caught anyone. In Germany, a high false positive rate was recognized, which can be the case even when someone has *not* forgotten things like keys, belts, etc. This, again, led to embedded bias and huge costs. It was a political problem. The technology is more effective in terms of detection, and despite its cost is meant to provide more security. There is no proof of that security, and furthermore the machine's capacity for image memory has been removed. There is a lack of data that leads to incapacity to determine the probability of attacks and no way to determine the impact.

Salter argued that – as a framework – risk management was impossible to apply. The core dilemma at the intersection of technology, security and perception is that – even if the millimeter wave scanner is technologically better – the privacy invasion is enormous. In particular, the measures that were installed to meet the privacy concerns subsequently undermined the capacity of the authorities to reveal the efficacy of the technology. So in order to protect privacy, they sacrificed the case for providing more security. The argument was that: "risk management is no longer the framework we are going to use in order to either make choices, or buy technology, or convince the public. What we'll do instead is talk about a security culture". There is an idea to promote a *security culture* in all aspects of aviation security. Rather than focusing on behavior and procedures, the new focus was going to be security values and awareness. Incidents were no longer to be seen as failures of the system, but rather learning events. This stems from security management systems in airports, where every time a part of an airplane fails, then that failure gets logged and databased. Over the past two years, within the aviation security system, however, there has been an attempt to learn from security incidents rather than hiding them as failures of the system. Salter gave Malaysian Airlines as an example. That organization had to fundamentally rethink how they did risk management after its multiple tragedies.

One of the primary ways that the use of these scanners is being explained to Canadians is that to protect passengers' privacy, the scanner uses a generic figure that indicates required additional search. What the Canadian Air Transport Security Authority (CATSA) is doing is to educate the public about this particular technology and to ensure them in terms of privacy rather than in terms of security.

Salter concluded by presenting some lessons to be taken from the millimeter wave scanner with regards to the LASIE project, from the adoption of more efficient technology in a public setting where there is uncertain knowledge. Firstly, the proportionality argument was not sold well in any circumstances, neither to Europeans nor Americans, or Canadians. Secondly, publicity made a massive difference in terms of public acceptance. Reactions to the "naked" images were severe, and it took a long time for the governments to come back from that. It seems to be really important that there is a good communication of both risk and reward in terms of this invasion of privacy. Looking at public

acceptance numbers for the millimeter wave scanner, people are much more willing to accept it now, since they see that object generated is the generic ginger-bread man. Salter's concluding point discussed privacy-by-design – the idea that one embeds those principles into any surveillance technology – and he stressed that although privacy-by-design had a good public effect, it also had the effect of undermining the capacity of the scanner to engage in certain kinds of activity, like verification.

Comments from discussants

Following Salter's keynote speech, two invited discussants were given the floor to provide their comments, reflections and any question to Salter.

The first discussant was Dr Petros Daras, a Researcher (Grade B) at the Information Technologies Institute (ITI) of the Centre for Research and Technology Hellas (CERTH), and a member of the LASIE consortium. Daras asked how the scanners could be used further, and in different ways that may be useful given the better technology. Daras asked Salter if it, for example, could be used for face recognition, to improve the bad quality of the pictures in the already existing systems. Daras' second comment reflected on why these scanners were only used inside the airport complex, as opposed to their usage at the entrance.

The second commentator was Dariusz Kloza, a Researcher at PRIO - and the team leader therein for the LASIE team – and Researcher at Vrije Universiteit Brussel. Kloza started off by underlining the importance of the change, i.e. the profound change that society has undergone from risk management being used as a tool, to an entire culture of security, as reflected on by Salter. This is comparable to the discovery of a 'risk society' or 'surveillance studies'. Yet people do not often realise this change of paradigm.

Kloza proceeded to stress the notion of proportionality. Legal scholars consider three factors that contribute to proportionality: 1) suitability, 2) necessity, and 3) non-invasiveness. Yet proportionality is often being narrowed to mere 'proceduralization' or formalization. We have started asking: does the society accept it? Does it protect privacy? Has the process been carried out according to the plan? These questions – themselves important – have replaced the more important question of whether we really *need* it. There is no data that the millimeter wave scanner helped threat detection at all, so what happens was the question was asked whether people were property informed, etc. In that sense, it became 'formal', as opposed to 'substantive'. Without an empirical 'use case' (i.e. substantive, proportional argument), this is the creation of a 'security theatre' (i.e. formal, procedural phenomenon).

Kloza further brought up the concept of privacy-by-design. He held that we still don't know how to use it in practice, and even when we do use it, it does not necessarily work. Salter already mentioned that privacy-by-design made it impossible to verify the accuracy of the body scanner's 'decision'.

Finally, as a conclusion, if we don't present a use case for the technology, like the LASIE "gadget", there is no point in developing such a technology. If we have no data it does do any good in the society and – even if we stick to risk management: "no data, no risk management". Thus, if we cannot prove any substantive proportionality of a given technology, asking solely procedural questions is not a solution.

Salter's response

The cases where face recognition has been integrated into other systems are e.g. entry/exit points to Superbowl, but that was seen as a huge invasion of privacy. The entire strategy is to isolate the screening process for objects, not for people – to remove any suspect of profiling or any policing away from the screening point. Risk management is a result of 9/11, the body scanners are a result of the underwear bomber and so on, so it is a very *reactive* system. Airport security, like many other security architectures, always chased the latest failure. In 1970s, the largest threat was hijacking, so the magnetometers were used to detect guns at the gate, and you could therefore walk right up to the gate. Then security points were moved further out towards the edge of the terminal and then even further. For example, at the Ben Gurion Airport, security processing starts while passengers are still in line, before they check-in. However, moving the checkpoints further away essentially only displaces the threat. In response to Kloza's comment on proportionality and proceduralization, Salter commented that the Canadian Government argued, back in 2001, exactly what Kloza did in his intervention. Items that are prohibited and discovered are usually benign.

Discussion and questions from the audience

Questions were taken from the audience, and the threat of non-travellers at the airport, such as the pilot, was brought up. Salter underscored that this is about the rationale behind who you study and in what way. Pilots are checked for criminal background, but there are no systematic screening testing narcotics or alcohol levels. In a similar vein, cargo does not get the same screening as other baggage. A question about whether it be fruitful to simply move the screening point further away from the central airport, e.g. at the very entrance of the airport. Salter underlined the importance of mobility rights. If, at the airport check-points, one is tested for example for previous criminal record or alcohol or drug levels, then they become a place where you go through a screening of things irrelevant to your right to mobility.

One member of the audience brought up measurement within the context of the security culture, to which Salter recapped his point about learning from incidents rather than registering them as failures. Safety management at airports has traditionally been to log all breaches and then create a failure database. Part of the security culture has been a different kind of recording information – again, viewing them as incidents to draw lessons from rather than labelling them as failures. Most likely they are going to keep measuring, but the way that they will do so is going to be different, and perhaps more constructive.

A final question asked which types of checks and balances can be applied so that surveillance can be done effectively and that it does not impose too much on privacy. Salter rhetorically asks how far we are from a kind of terrorist profiling. The biggest threat that aviation security people talk about are not 'known travellers' but 'unknown travellers'. Because of the framework of risk management, unknown people are the most dangerous. Salter concluded by reminding the audience about the distinction between risk management, which is about quantification and profiling, and a security culture, which is about broadening what/who gets counted as a security risk.