The Congress
Le Congrès
CONGRESS OF LOCAL AND REGIONAL AUTHORITIES
CONGRÈS DES POUVOIRS LOCAUX ET RÉGIONAUX
1949.2019
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CEEE|Gov Days 2019

Central and Eastern European e|Dem and e|Gov Days 2019

Cyber Security and eGovernment

2 - 3 May 2019, Budapest, Hungary

Keynote session II

Statement by Martin Fodor

Congress of Local and Regional Authorities of the Council of Europe

Cyber security and e-government. Keynote session III
Statement by Martin Fodor - Congress of Local and Regional Authorities of the Council of Europe

Colleagues, Ladies and gentlemen,

It is always a pleasure to be back in this beautiful city of Budapest. Some of you will remember me from last year, when I came to talk about smart cities. I like to think that I can't have been that bad, or you wouldn't have invited me back.
As the rapporteur for the report on smart cities, that the **Governance Committee** is now preparing for the Council of Europe Congress, I was tempted to speak on this topic again today, but of course the theme of our conference this year is "cyber security and e-government", so I will focus on that instead. I am a city councillor in Bristol in the UK. **So why should a city councillor be interested in cybersecurity?**

I do not need to remind you that the world we live in is evolving rapidly. Maybe too rapidly. New technologies are changing our way of life. More and more of our activities are becoming virtual, or digital. Our smart phone is now our best friend.
Is everyone here listening to me as I give this speech? Some of you are paying more attention to electronic devices, I know I do this. Our attention span is shrinking, just as glaciers are melting in the arctic. We are living in a connected world and we find it increasingly difficult to disconnect. Take a look around you next time you are in town.

Everybody is clutching a device, typing as they walk, not looking where they are going. They have wires coming out of their ears, they cannot hear you. I'll just put my smartphone back in my pocket and ignore the alerts. But do you feel safe? Welcome to the world of the smart-phone zombie!

Just last month my council offered all politicians training on personal security - much practical advice. But the newest section we cover is on **IT security and online communications** – how to be secure with private council data and residents' data, plus how to be safe online. There were plenty of warnings about our use of social networks and the risks of privacy being exposed – which can lead to real life threats against us if residents or political opponents get angry. Our last session of Congress in Strasbourg in fact had a debate about the risks to Mayors under pressure from opponents. Online hostility can escalate into real life, and political debate is getting more polarised.

Talking about safety, what about surveillance? Or rather: 'mass surveillance'. The latter is the perfect example of the misuse of new technologies. Big brother really is watching us. This is not science fiction anymore. It is a reality. **As we walk around my city some smart phone boxes are tracking us to offer free wifi, but also perhaps, to target adverts as we pass local businesses. This has been quite controversial. The vast number of cctv cameras the council operates can also track faces as they move around the city – it's something the Mayor joked about, but it worries some people. We welcome security cameras when there is an incident where evidence is needed, but most of us are uneasy that our daily movements can so easily be tracked.**

It's a world where online communication can and is being collected, internet history retraced, and phone calls monitored. A world where the security camera that you buy to protect your home from burglars can all too easily be hacked to spy on you. A world where virtual assistants can record your private conversation, not just switch the music on. A world where, thanks to cookies, web servers know you better than you know yourself.

By accessing and sharing our data, for the sake of "our safety", governments and corporations are playing a dangerous game. You may feel physically safe, but your personal data, meaning your privacy, does not belong to you anymore. Hence, one of our fundamental rights is being violated. I said last year that as a local politician **I am a data controller**, and have had mandatory training to ensure I manage data legally. I cannot build up all the contracts I make into a database without express permission now. But **more than a legal issue, this is an ethical one**. I will not go any deeper into the debate on privacy versus security, but I would just point out that the "Internet of Things", which was supposed to bring people together, has actually made them more distrustful: distrustful of their governments, who they think is studying how they use energy at home through their smart meters, for example, but also, more importantly, distrustful of other people. We are growing further apart.

How many of you have already received a “phishing” email saying that your device has been hacked and that you should pay some technician to fix a problem that does not exist? I used to receive a call every week claiming to be from the Windows server room concerned about my operating system security – which was odd as I had no windows computer.

Or an email informing you that you have magically won some lottery and that you need to give your bank account details in order to receive the money? How many of you have heard stories about identity theft? I hope not too many of you, but on average 1 in 5 people lost money to an imposter scam[1]. My city has some of the best digital connectivity with a well connected young population – and one of the highest cyber fraud levels in the country…. More dependence can lead to more carelessness or risk.
In 2017, the amount of reported loss to impostors was 328 million dollars in the USA. Pretty lucrative business don’t you think? And billions have been lost to all types of scams.

So why take the risk of stealing the mobile phone or the purse of someone in the street when you can extort money from many people from your sofa? Why risk physical violence or getting caught, when you can hide behind an **untraceable IP address, and remain anonymous**? More and more people are exploiting these possibilities and online scams of all kinds are now commonplace.

Older people are vulnerable, too. According a report from the Federal Trade Commission, in 2017, the average loss – from cybercrime - for people aged 80 and over was over a thousand U.S. dollars, whereas, for people aged between 20 and 29, it was just 400 dollars (which is still 400 dollars too much). Millennials might be more frequently victims - since they are spending far more time and doing almost everything online, compared to their elders - but they are also more likely to report them. So **as service providers our organisations are expected now to offer all possible services in a digital form,** but at the same time we have a duty to try and make all these transactions secure, and warn people about the need for security.

What can we do against this virtual menace? Several initiatives have been put in place in order to raise awareness against online scams and to support the victims. Many websites have been created to provide online assistance. To mention just one of the thousands that exist, the website “have I been pwned.com” help users ensuring their personal data have not been compromised in data breaches. But for those who are less tech-savvy, and who prefer face-to-face conversation, some non-profit organizations are also very active. The Identity Theft Resource Center in California, for instance, proposes training, and presents “good behaviours” we should all adopt to reduce the risk of identity theft.

[1] Based on the data from 2017: https://heimdalsecurity.com/blog/top-online-scams/

The climate of mistrust that I am talking about is also due to the rise of fake news and information warfare. Social media have created a new public space for public discourse. But instead of uniting and informing people, they are dividing and misinforming them. They are dividing people by spreading hate speech. Some people are being excluded and marginalized, and the quality of our democratic debate is, as a result, declining. All too often, such media misinform us and are used as weapons to manipulate public opinion. Modifying the reality by not telling the facts as they are, but as you want them to be, has become a common practice which can have enormous consequences. Just look at the impact of such media on the Brexit issue.

Hence, social media, which were once seen as the ultimate democratic tool, also serve the aims of undemocratic forces. It is almost Orwellian, the way that some countries have begun to use social media to hunt and trap dissidents. It is also shocking that police forces in Egypt are using them and dating apps to trap gay people. These virtual means of communication and spaces of free speech are, in fact, restoring censorship and **facilitating the persecution** of targeted groups of people.

The quality of our democracy, or maybe democracy itself, is at threat. We cannot let the technology take over. New technologies are changing our way of life. For better and worse. They are a double-edged sword. The way we use them - **and how we programme them -** will reflect the kind of future we want for our society. Hence, we need governance – **we need to be able to take informed decisions** – to be able to choose how we want to live our lives and not get sucked into some Brave New World where we become the slaves of artificial intelligence. So one question is: who writes the Apps? The way they are designed does affect what they do and who they serve. I hope it’s not just teenagers in California who want pizza delivered really efficiently.

This is why cybersecurity is so important. The Council of Europe has already integrated it into its field of action. It has produced the first- and only- binding international instrument on cybercrime, known – you might like to know - as the ‘Budapest Convention’ (as it was opened for signature just a few hundred metres from here in 2001). This has now been ratified by 63 countries, comprising not just Council of Europe member States, but also non-member states such as the USA, Canada, Japan, Tonga and Paraguay. This diversity shows well that cybercrime is not a European issue, it is a global one. The Council’s action does not stop here, since it has set up a Cybercrime Convention Committee in order to facilitate the use and the implementation of the Convention. Finally, a Cybercrime Program Office has been created in order to assist countries worldwide in strengthening their legal systems capacity to respond to cybercrime threats.

We need to prevent cyberattacks, but more importantly we need to protect our data, and by extension people’s privacy, our privacy.

The most embarrassing event recently for my council, you might like to hear: our citizens panel, who we consult about their opinions on many issues, were recently sent an email about the council's control of their data under the EU GDPR – the general data protection regulation. But the whole mailing list was sent out copied open, not blind copied! So all emails were exposed to all the panel. Very careless!

I return to the question I asked at the beginning of my speech, why do I feel concerned about cybersecurity? Well it is because for me it is about securing people, and as a Green Party councillor I am accountable to my residents. My duty is to safeguard their rights and security whilst making sure they all feel included and listened to.

Councils too are now using a wide range of new technologies. And **councils too are the targets of cyberattacks**. According to a 2017 study conducted by the campaign group Big Brother Watch, UK local authorities have experienced 98 million cyberattacks over five years. Put differently, this means that there are around 37 attempted breaches of UK local authorities every minute. Even though the prevalence of cyberattacks varies depending on the city and the country, we all need a healthy level of cyber security. It is essential to ensure that our public services are kept and running, and to prove to our citizens that they can **trust their city councils** with their information.

Now, what can local and regional authorities do about it? In 2015, the UK Department for Communities and Local Government released a report entitled "**Understanding Local Cyber Resilience, A guide for local government on cyber threats and how to mitigate them**". Apart from presenting the various threats local authorities may face, the report invites them to adopt the so-called **10 steps to cyber security**. By doing so they will eventually reduce their vulnerability to these same threats.

Besides, only if we are cyber resilient will we be able to implement e-government. I highly value e-government initiatives because they improve government processes, they connect more citizens in more ways and they build external interactions.

In my city, residents can access a wide range of public services from our webpage. From getting a residents' parking permit to reporting a street issue, they can easily be informed of what is going on in their community. Well-informed people can actively participate in society. And if people participate, they will feel empowered and included. This is what matters to me at the end of the day, that I work to build a society which leaves no one behind. It is fundamental to achieve social cohesion. Being a city councillor and Green I want to serve all people, not just those with the latest smart-phones. As I see my city becoming increasingly innovative and digitalized I am becoming more concerned about the **inclusiveness issues** for those left unconnected. We only have a single customer service point now in Bristol, and it's a very expensive bus ride from some parts of the city.

We have asked for a skype access option, which could be made from libraries or other places, but this is not available yet.

As I said before, more and more services are digitalized to facilitate their access. However, when it comes to new technologies, we are not all equal. **Some groups of people may feel marginalized because they are not tech-savvy**. Today's kids know how to use an I-pad before they learn to walk. Older people, on the other hand, are not so able to keep up with the march of technology. We have to make sure that we do not leave people behind**. E-tools - both for services and for democracy - must be instruments of inclusion not of exclusion. <u>They must be complementary, not a replacement for existing channels.</u>**

I'll conclude this speech in the same way as last year. For those who were here and who heard it last time - no spoilers please. In the same manner that we need to "keep people at the heart of smart cities", **we also need to keep the people at the heart of our cyber resilience initiatives**. The principles of speed, efficiency, and practicability – however much they are favoured by our institutions and appreciated by the public – must never prevail over people's rights. We may be living in an e-democracy, but we should not forget that in this compound word, it is the "electronic" which must serve democracy and not the other way around. We are here to serve people. Safeguarding their rights and their security is what matters. So, let us keep in mind that in an increasingly digital an inter-connected world, cybersecurity is not an option, it is a necessity. And let us remember our that values and rights are worth fighting for. Let's not forget our humanity in a society which is increasingly relying on artificial intelligence. Let's make the technology work for us all.

Thank you for your attention.