Security and Digital Surveillance:
A discussion with Christopher Soghoian and Ben Hayes

After the Paris attacks of November 13, 2015, debate has again flared up around the use of (digital)surveillance by governments and intelligence services as a means to prevent terrorist attacks. As fear of terrorist attacks seeps into politics and popular consciousness, voices can increasingly be heard advocating for fewer legal boundaries to be put on digital surveillance: governments should be able to use all means necessary in 'the war on terror'.

We find ourselves at a crossroads. Digital technology holds more possibilities than ever, yet it seems that violent extremists extensively use digital means to communicate and plan attacks. The choice of more invasive and broad digital surveillance methods then seems obvious. But do we realize the effects this will have on society?

On November 10, 2015, Human Security Collective, in cooperation with Dutch Coast and Partos, organized a conversation on digital surveillance and security. Discussing the issue and sharing their thoughts were activists Christopher Soghoian and Ben Hayes, who follow critically developments in government policy concerning digital surveillance, technology, security and human rights. Lia van Broekhoven of Human Security Collective moderated the event.

According to Soghoian and Hayes, enabling the expansion of digital surveillance will have – and is already having – a profound effect on society. The 'war on terror' has been, as they argue, a driving force for the creation of a 'security paradigm'. This paradigm can be seen as *the* dominant political discourse, which seems to frame nearly everything in terms of security threats. The increased use of digital surveillance is, according to Hayes and Soghoian, an additional development that has further promoted the dominance of this security paradigm. In fact, these factors have led to the creation of a 'security state', which directs much of its attention towards cancelling out and, of course, investigating what it deems as security threats. For instance, much of the resources spent in dealing with the current refugee crisis in Europe are used on screening incoming refugees, instead of creating an enabling legal environment for people wanting to seek asylum. As Hayes emphasizes: "The current refugee crisis is because of the securitized response of the government against migration. The problem is only partly because of the numbers coming in".

The security state is thus built on a paradigm that tells us that almost everything is a security threat, justifying the expansion of even broader surveillance strategies. Furthermore, the fact that digital surveillance has become a cheap option for governments forms a facilitative environment for the expansion of digital surveillance. As Soghoian said, "Because of technology, surveillance has become

so cheap, that it is the first thing governments do, instead of a last resort". The possibilities for collecting so-called 'big data' therefore are now immense.

But, as both Soghoian and Hayes emphasized on the evening, a paradox is at work in the security state. While governments actively advocate for more digital surveillance in their efforts to counter terrorism, it is not clear to what degree broad surveillance methods actually 'work'. The Paris attacks have regrettably highlighted that governments cannot rule out all risk. Are the methods used – primarily mass-surveillance – really that successful in preventing terrorist attacks? Or is, because of its broad nature, everyone a potential suspect, which in turn impairs governments in singling out 'real' subjects? Though targeted surveillance may in fact be of key importance in preventing attacks, the effectiveness of mass-surveillance is highly questionable.

The value attached to digital surveillance is, according to Hayes, not realistic. Politicians who advocate for increased surveillance measures in their pledge to stop at nothing to prevent terrorist attacks are, in fact, making a promise they cannot keep. At most, a false sense of security is created, while placing individuals and civil society organizations under increased scrutiny. As Hayes said: "The agenda here is mainly driven by political window-dressing". The negative consequences of mass-surveillance for both individuals and civil society organizations are numerous – from the threatening of individual privacy to the compromised operating environment for civil society organizations.

Civil engagement and activism against mass-surveillance is thus of critical importance. Soghoian addressed the fact that: "These measures are implemented without any form of democratic process. We should come to mass-surveillance and police hacking *after* such a process. Now this liberty is just taken". Civil society is key in creating an opposing force to governments who adapt laws meant to protect individuals and civil society organizations in order to put in place mass-surveillance without due democratic process. Both civilians and civil society organizations need to voice their criticism on digital surveillance in order to raise public awareness – both because it is such an important issue, but also to raise the lid on what their governments are doing behind closed doors. As Hayes said: "Civil society is the only thing that can protect us where laws cannot, and politicians will not".

Learn more

Ben Hayes (biography and links to work): https://about.me/ben.hayes
Ben's Ted-talk: https://www.youtube.com/watch?v=Pj6TyN35GlE

Christopher Soghoian (biography and links to work): https://www.dubfire.net/
Christopher's Ted-talks: https://www.ted.com/speakers/christopher_soghoian

Write-up by Dorine IJsseling