Infosecurity

(Gran knows why)

by Arjen Kamphuis

A collection of articles, posts and lectures

And a handy InfoSec guide

Infosecurity

(Gran knows why)

by Arjen Kamphuis

A collection of articles, posts and lectures

And a handy InfoSec guide

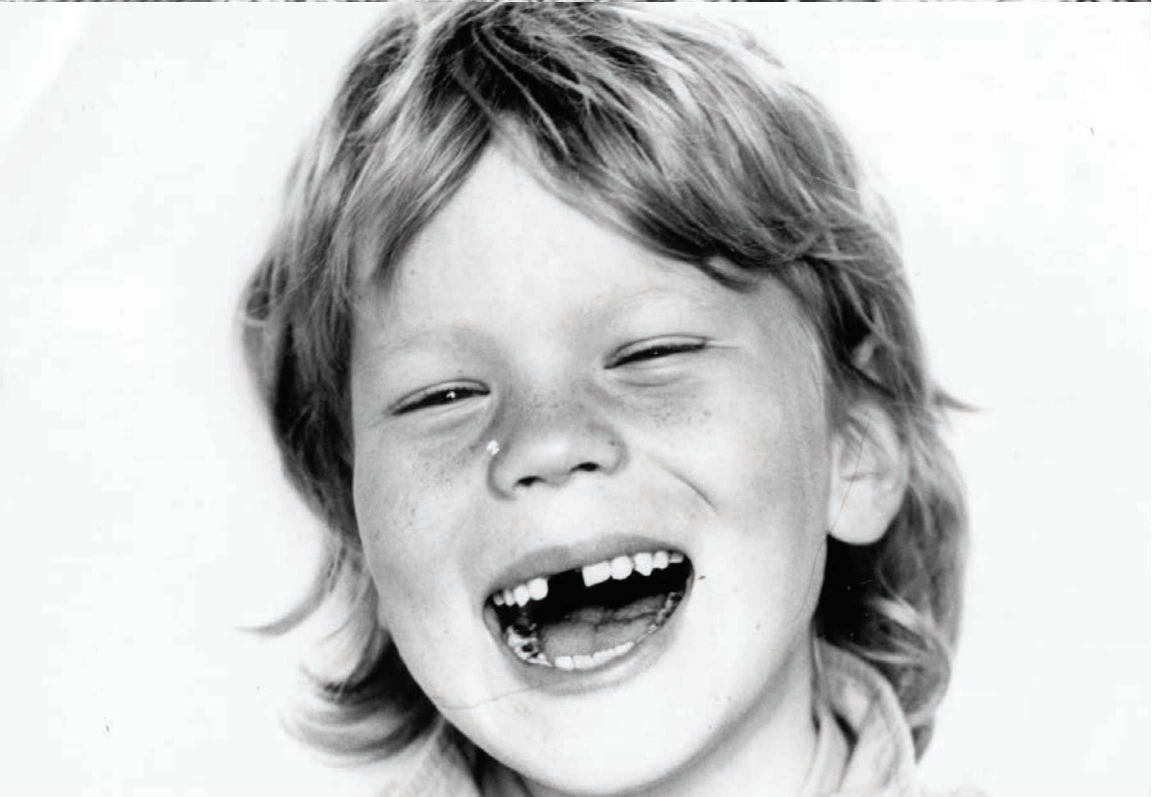
Colophon

ISBN 9789090328218
First edition, 2020

Infosecurity (Gran knows why) - By Arjen Kamphuis
A collection of articles, posts and lectures. And a handy InfoSec guide

Initiative by #teamArjen: Ancilla van de Leest, Sanne Terlingen,
Jos Weyers, Maurice Verheesen, Helma de Boer

Editor: Helma de Boer
Preface & photo selection: Ancilla van de Leest
Book design & layout: Harry van Mierloo
Cover design: Ancilla van de Leest & Harry van Mierloo
Photo back cover: Jos Weyers
Publisher: Gendo
Print: Bookadew, Roermond



493
LEGO
6 years & up

Preface

The book you are holding was written by a man who has disappeared. It was compiled by people who loved him, and who feel the need to fill the void he left with a lasting echo of his work.

If Arjen would stand before you right now, he would leave you no choice but to quickly develop an opinion on him. This could be positive or negative – depending on your own biases – but he always left an impression. With his strong voice, black humour, quick wit and straight forwardness on complicated political issues, he set out to challenge the status quo and speak truth to power. It was no surprise he was a well sought after lecturer at schools and at companies. He was a talented and passionate debater, with a stunning memory for even the most minute details of past events.

It was not just his passion and brains that got him noticed. Arjen wore his trademark 'nerd look' with pride: long blonde hair and black attire. He often bought a couple of those same pants and shirts at once, so as to never run out of his uniform. By fully embracing his geekiness, he made an effort to be a good ambassador for his fellow nerds, as well as the hackerspaces they inhabit. Quirky hackerspace Hack42, located in an old military base in Arnhem, was his home away from home, where he was even welcome to stay the night whenever he was in the neighbourhood. The white church next to it is therefore an appropriate pick for the launch of this book, around the time of his birthday.

As a young and optimistic futurist, Arjen was convinced technological advancements would allow for a better humankind and healthier planet. However, over the years he became increasingly dismayed that other people did not seem naturally interested in the bigger picture for the better world he clearly envisioned technology could bring us. The lack of knowledge and insight that powerful people displayed, baffled him. After all, wilful ignorance borders on the side of criminal when making decisions that affect all of society, he argued.

Principled, passionate, outspoken and energetic, Arjen became aware of and vocal about the fact that society is using technology in clueless ways. Always way ahead of his time, he preached inclusivity of everyone early on. If his writing and speaking had one message, it would be that. Let's not let slip this opportunity of advancements in technology to make lives better for everyone in the world.

A true renaissance man, he certainly enjoyed being a bit of a provocateur in conveying his message. And, as you will soon come to read, he did not shy away from making bold statements in order to wake people up to the disconcerting reality he perceived to be unfolding right before our very eyes. But as arrogant as he would come across when on stage or engaged in a heated debate, as gentle and humble a soul he was when out of the spotlights.

Always on the lookout to make himself useful, and help people with his vast amount of knowledge, as well as his appetite for physical labour. When he was not handing out customised surveillance-proof laptops to befriended journalists and hacktivists, he was supporting crowdfund campaigns for innovative technology with the same enthusiasm he put into constructing hiking tents or Ikea furniture. He would never throw away a sleeping bag, because 'you never knew when you'd have a bunch of people over who were in need of one'. Indeed, when friends or strangers alike needed a place to stay for a night, or even a few months, he would not think twice to quickly provide a roof over their heads. He was a giver, without expecting payback in glory or otherwise. It was not unusual to be gifted a book by him he thought you would like. Many a friend still calls him a mentor, too. Some say he was a dreamer.

Arjen loved sailing more than anything, and his big dream was to one day own his own sailing boat. His friends associate him with a diet of fish and a sip of the occasional quality whisky. He loved to travel, and when he was young, he would regularly go hiking in snowy mountains and other rough and unusual places. In later years he would allow himself to enjoy more luxury holidays and not 'having' to do too much. But whenever the opportunity arose to plan for a boat trip, he would always jump to the occasion.

His last holiday to Norway was right up his alley: cool temperatures, raw nature and plenty of solitude. He joked about the possibility of being eaten by a polar bear, because "Really, it happened to a couple of tourists not too long ago".

How does a person as unique and fascinating as Arjen come to be? We know that much of his intellectual disposition and broad interests came from the middle class family he was born into. His mom was a psychotherapist, his dad worked as an ergonomist for a large tech corporation. In naming the book 'Infosecurity (Gran knows why)', we half jokingly say Arjen's grandmother was his big inspiration, and indeed it appears like his principled and engaged attitude came from his family. A love for technology, society and the outdoors were instilled in him from a young age. Many of the childhood pictures included in this book show a boy who engaged in activities he still enjoyed later in life: building things, being outdoors, sailing a boat and checking out technology from up close. His younger sister and him seemingly lacked nothing growing up.

The fall of the Berlin wall was a life defining moment for him, as it undoubtedly was for many of his generation. The event left a great impression on him, one of hope and liberty that he carried with him in everything he did. In matters of the heart, his long-term relationship with the beautiful and articulate MI5 whistleblower Annie Machon, was formative to his life and work, as well. Yet not all of his life was rainbows and unicorns.

His beloved mother suffered from Parkinson's disease when Arjen was only a teenager, and her decline and eventual euthanasia in 2007 made a lasting impression on him. We can only speculate whether his simultaneous struggle with academic results was a result of this tragedy, but the suffering of this strong, wise and caring woman certainly broke his heart.

Another tragic and traumatising event occurred when Arjen was a young adult. He was involved in a serious mountaineering accident in Argentina, in which a several of his hiking partners lost their lives right before his eyes. He did not speak about the accident much, but did confess once that the guilt of not being able to save them still haunted him. Another consequence was that he was unable to fully pursue his passion for dangerous outdoor adventures due to a permanently injured knee. He continued to suffer from the physical pain until shortly before his disappearance, when he proudly got 'upgraded', as he called it, with a titanium part. Even when he painfully chopped off a fingertip or two during wood chopping - as one does - he still kept his cool. "All the better!" He would joke sarcastically, "One more way to make it more difficult for authorities to track me through fingerprints!" His dark humour will be so very dearly missed.

Never one to display any sign of discomfort, Arjen struggled to be open about even the most obvious personal flaws or hurts. He was here to save the world, after all. A strong shoulder to lean on, and super heroes do not show weakness. At least not when in costume. But as much as he was loved by those around him, he too, was all too human. Despite his career success, financial challenges caught up with him repeatedly. And it is entirely possible he lost a good friend or two, simply by being a no-show to obligations now and again. No surprise then, that when he initially went missing, alarm bells did not immediately go off with his inner circle. "Just like Arjen," we thought, "to stay on holiday for a bit longer and forgetting to get in touch".

Arjen's disappearance caused quite a media storm. Many dozens of people across Europe reported they thought they had seen Arjen, but not a single shred of evidence has resulted in finding Arjen. After a year of thorough investigation, for which we are grateful, Dutch and Norwegian authorities have closed the case, assuming he was probably killed in a kayaking incident. Until 'new shit has come to light', this is where the story ends. But without finding any actual bodily remains, what actually happened remains a puzzling mystery. A painful open ending for those who held Arjen dear.

This book is a labour of love. A love for Arjen as a person, and a love for all he did to create a better world through advocating for ethical choices in technology.

Arjen has left plenty food for thought, through all of his accumulated words. We are convinced the world will be a better place when his knowledge and wisdom are shared with a broader audience.

If you are one who sees the importance of digital rights, please take it as an invitation to incorporate wise digital choices in your life, and to further spread these ideas in your very own way.

Arjen was truly one of a kind. We are grateful for his relentless contribution, unmatched wisdom, never-ending encouragement and warm-hearted company. On the off-chance that we are experiencing a self-chosen disappearance* and he chooses to resurface, Arjen could expect to get kicked in the nuts, receive a couple of bear hugs, and to be sat down and asked about his interpretation of current affairs.

Arjen,

you are

#stilldearlymissed

#TeamArjen

Ancilla van de Leest
Helma de Boer
Jos Weyers
Sanne Terlingen
Maurice Verheesen

And special thanks to Harry van Mierloo

[*] It has come to our awareness some people are drawn to Arjen's story through their own wish to 'disappear'. If you are contemplating anything like a self-chosen disappearance, please know we want you to stay. You can get help through various local foundations that have people ready and waiting to help anyone with depression. In the Netherlands the suicide prevention hotline number is 0900-0113

Arjen Kamphuis and the public cause in the digital world

JANUARY 7, 2020 – BY BART JACOBS

In the beginning of 2014, Arjen Kamphuis was interviewed by the online channel London Real. When asked whether he considered NSA whistleblower Edward Snowden a hero, Arjen answered:

"I think he is a hero in the sense that he very consciously made a choice to make his own life a hell of a lot more difficult for a greater good."

We may say that this description applies equally well to Arjen himself. He too made his own life more difficult due to his outspoken and principled attitude. He was largely driven by the public interest. He had a compelling way of talking, sometimes unrelenting but he was dedicated and involved, and he was almost always right. Now that I am writing this, I see him jump to life, look at me with his piercing eyes and ask me compellingly: tell me, on what topic was I not right then?

Arjen was committed to the public cause, in particular in the digital world, where he emphasised the close connections between several topics:

protection of fundamental rights, open source software, in particular in the public sector, security and sovereignty, surveillance and privacy, abuse of power by governments and companies. In this introduction I give some background information on these matters, from the perspective that what Arjen was committed to, is still very topical. I regard him at least as a 'Dutch hero'.

Within computer science, the field of computer security plays a special role. While most computer scientists are focused on nice things you can do with computers, the focus of computer security is not on such desired functionality, but more on what nasty things can be done with computers: for example, breaking into your laptop to steal (personal) data so that the attacker can impersonate you (identity theft), or intercept your communication to embarrass you, or to uncover your journalistic source, or to lock you up as a dissident. A professional form of distrust belongs to the field of computer security. Security specialists can often be recognised by that attitude. In every situation they think: what if he does this or that, then ...; are we prepared for that, and how do we recover after a (partially) successful attack? Such an attitude can be unwelcome or exhausting, but it has shown to be vital in today's digital world that such people are there and that they are taken seriously, for example when, once again, for ill-considered convenience, it is suggested to vote digitally.

More generally, computer security is about regulating access to assets, ie about regulating access to digital matters. It has always been this way - but in our modern society stronger than ever - that information gives power: if I know certain things about you, I can use it in a positive or negative way to influence your life. This is all the more true for a state that knows a lot about its citizens and has the monopoly on violence to make that knowledge and power very concrete. Engaged specialists in computer security, such as Arjen Kamphuis, are strongly aware that the regulation of digital access is directly related to the balance of power in society. That is why they like to engage in political and ethical discussions.

Software tells a computer what to do. Many security issues arise when that software contains programming errors, or secretly does things that are not intended. The best remedy for this is to make the software open source. This means that the source code that the programmer typed in is made public, so that in principle everyone can see for themselves how the software works. The idea is that hidden back doors with unintended functionality become visible to, and that any errors can be detected by, experts who check the software. The open source concept also means that anyone can use publicly available software at no cost. Important software (Linux, Apache, etc.) is open source and plays a crucial role in the global IT infrastructure. Companies are often less keen to make their software open source, mainly because they are afraid that this will make their working methods public and that these methods can be used and taken over by others. This argument is increasingly losing momentum as IT revenue models are based on cloud-based services and not so much on selling software. Organisations that continue to stick to black-box (closed, non-open, proprietary) software therefore, rightly, evoke increasing mistrust.

In 2002, the Dutch Parliament adopted the Vendrik motion, which encourages the government to make systematic use of open source software. This led to the government program OSOSS: open standards and open source software, which, however, did not really get off the ground due to active opposition from the commercial sector and due to a lack of support and commitment within the government itself. Arjen Kamphuis has been involved with these developments, vocally and actively, and was both angry and disappointed about the lack of a breakthrough of open source software, for various reasons.

- For ideological reasons, he thought that all software used for a public task should be open source because, according to him, (public) power should function transparently. This is and remains a strong point that originally also formed the basis for the Vendrik motion, but was never really picked up and continued politically.
- Arjen really couldn't understand why the Dutch government spends billions on commercial software while free open source software is available - or can be developed if necessary. These large expenditures continue year after year due to the lock-in that comes with black box software, which means that the government cannot go anywhere else. I think that Arjen has been a little too optimistic about the effort it takes organisations to switch to open source software and therefore have to take more control of themselves. Public organisations in particular prefer to buy off risks via an external supplier rather than to get actively involved with something as complicated and elusive as software - and therefore run (administrative and political) risks themselves.
- According to Arjen, this local development possibility of open source software should be systematically encouraged, as an investment in the Netherlands (or in Europe), and not in mostly American commercial software suppliers. He did not shy away from talking about sovereignty, of the Netherlands or of Europe. This sovereignty argu-

ment has found more and more resonance in politics in recent years as it is becoming increasingly clear that Europe is in danger of being crushed in the struggle between China and the United States, including in the digital field. And indeed, with targeted investments in the development of open source software, Europe can build its own position and thereby guarantee that European values are anchored in software.

- In line with this, Arjen gladly emphasised that the use of open source software leads to better security and can also offer some protection against privacy violations through systematic surveillance by assertive intelligence services. The Snowden revelations have been a confirmation of what he always suspected, and a motivation to argue even more strongly for a transparent government that protects citizens.

He wrote about these points in a characteristic way: “Somewhere, the appalling scale of waste of money, the jeopardising of cyber security of the Netherlands and the violation of the privacy of millions of Dutch citizens is systematically condoned”. This formulation indicates an element of conspiracy thinking in his analyses, but also the realisation that he did not have a good view and grip on where and how crucial decision-making about public ICT takes place in the Netherlands. He fully realised that the issues that concerned him were great and that there were major opposing forces and interests. That is precisely why he has been fighting this ‘somewhere’ with great commitment and dedication.

Unfortunately, we must conclude that far too few politicians today recognise the strategic and geopolitical importance of this public cause in the digital world and have not made it their own subject. The drive with which Arjen kept them sharp, is sorely missed.

Bart Jacobs (prof. dr. B.P.F. Jacobs) is Professor
Interdisciplinary Hub for Security, Privacy and Data Governance
at Radboud University Nijmegen, the Netherlands

About Arjen

Arjen Kamphuis (Groningen, 26-01-1972 – missing since 20-08-2018, last seen in Bødo, Norway) was a cybersecurity expert and hacktivist.[1] He addressed topics like open standards and free software, safe elections and an IT-aware and IT-capable government, eventually to protect free speech and democracy. Ever since Snowden leaked highly classified information from the National Security Agency (NSA) in 2013, he was especially dedicated to protecting investigative journalists. He wrote the book 'Information security for investigative journalists'[2] with co-author Silkie Carlo, director of Big Brother Watch.[3]

Career

Arjen Kamphuis was co-founder and Chief Technology Officer of Gendo. Kamphuis studied Natural Sciences at Utrecht University and worked for IBM and Twynstra Gudde as IT architect, trainer and IT strategy advisor. He was a certified EDP auditor and information security specialist. Since 2006 he helped to secure the information systems of corporates, national government and NGO's. His work ranges from regular privacy-compliance

[1] *https://en.wikipedia.org/wiki/Hacktivism*

[2] *https://en.wikipedia.org/wiki/Source_protection*

[3] *https://en.wikipedia.org/wiki/Big_Brother_Watch*

and security-awareness up to countering espionage against companies, journalists and governments. To keep up technically Arjen was involved with the global hacker-scene. He kept in touch with (former)employees of spy agencies and other professionals who work at the front of critical infrastructure protection. He worked on the strategic impact of new technological developments and the social, economic and geo-political impact of science and technology.

In 2016 Kamphuis started working for Brunel in Amsterdam as Lead Advisor Information Security and from then on he worked closely with William (Bill) Binney and Kirk Wiebe. On August 11th 2017 he was invited with Bill Binney to a press conference in Austria, together with Max Schrems and Thomas Lohninger to talk about mass surveillance in Austria.[4] In late 2017 he started the Brunel daughter company Pretty Good Knowledge as Technical Director. Bill Binney and Kirk Wiebe were co-founders and they contribute as Directors of Analytics.

Kamphuis has been involved in formulating public IT policy in the areas of open standards and open source for the government and public sector. He advised senior managers and administrators of companies and public institutions, members of parliament in several European countries and the Dutch Cabinet about the opportunities offered by open standards and open source software for the European knowledge economy and society as a whole. In the expert team of Plasterk he advised about (not) using e-voting for elections.

[4] *https://www.youtube.com/watch?v=2-iJ_IZ0-y0 (27:18 - 34:32)*

Personal life

Arjen Kamphuis was in a relationship with Annie Machon, former MI5 intelligence officer and whistleblower, between 2007 and 2014, living in Düsseldorf and Berlin.[5] In 2016 he settled in Amsterdam. He travelled a lot because as a much sought-after international speaker on technology policy issues, Kamphuis gave over 100 keynote talks every year. He wrote about his insights and ideas for Huffington Post, Webwereld, Sargasso, Consortium News and Globalresearch. He was asked to contribute to several shows and programs, like London Real, Max Keizer, Russia Today, BNR news radio, RTL tv, Café Weltschmerz and TEDxDelft. For Reuters he trained journalists in information security throughout the world.

Disappearance

The Norwegian police conclude that Kamphuis probably drowned due to a kayaking incident on the fjord near Rognan, Norway. His body has not been found.

References

His videos can be found at his YouTube Channel.[6]

[5] *https://en.wikipedia.org/wiki/Annie_Machon*

[6] *https://youtube.com/user/arjenkamphuis/videos*

Contents

Part I: Arjen's philosophy

Part II: The InfoSec Book

Epilogue

Part I:

Arjen’s philosophy

1.

Defend yourself in this digital world. No one else will do it for you

MAY 9, 2018 TEDXTALK[1] – ARJEN'S LATEST BIG PODIUM

In late May 2008, a decade ago, there were many small supermarkets in Amsterdam that were out of fresh milk. This was not because of a cow strike, but because the mobile phone network had been down in the most of the Netherlands for two days. This was just after the introduction of the first iPhone – it seems forever ago – so most people didn't even notice. But many small supermarkets and small retailers were already using mobile data to run their logistics. So when the network failed, so did their logistics. No 3G, no fresh milk. This was not the first time we had big failures like that and it would also not be the last and I won't be the first one to tell you how important technology is.

System failure

When computers and networks fail, everything stops today. We have been very depended on electricity for decades, but certainly over the last 15 years computers and computer networks have become just as vital to keep us safe, healthy and of course in cat videos.

A how-to protection

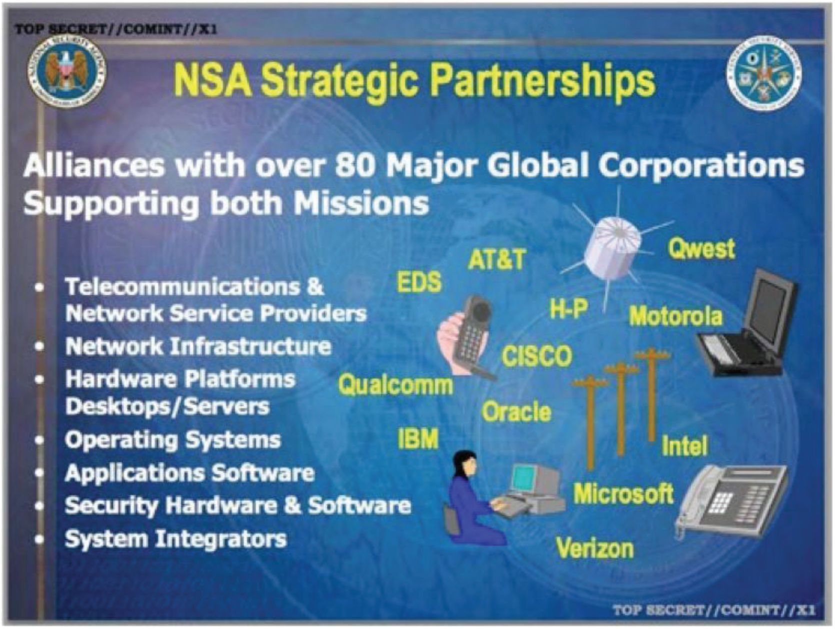
So, we need to be able to protect ourselves and the people around us and the places we love. This is one of the reasons why with a journalist friend (Silkie Carlo) I wrote this book, which is a free download online, to help train people to use open source security tools, to have privacy and anonymity when you need it and to keep a secret. I am a digital-defence instructor and I train activists, journalists, lawyers and people around the world who need to be able to keep a secret and to communicate securely to save lives. The book is intended to help non-technical people to be able to do that on their own. It's a free download in several languages and you are also allowed to reuse the text. So, if you want to make a version for 12-year-olds, go ahead, you don't need my permission.

Paying to be spied upon

To go a little bit into the problem, Europe buys the vast majority of its IT we run our lives on from abroad. US software and services. Chinese hardware. Not only this is costing us something like 250 billion a year – which is a couple of million jobs we don't have in Europe – it also means that we buy technology that is vital to us every second of every day what we have no control over, we don't know what it does on the inside and all kinds of bad things could happen and indeed have happened. Thanks to a series of courageous whistleblowers, of which Snowden was one of the more recent ones, we know now for sure that this stuff is being abused against us. All the time. China, the USA and many other countries have espionage interests against Europe, so these things are being abused against our political and social interest. Of course there is also a lot of economic espionage, meaning more money, more economic growth and wealth that we don't have in Europe.

Bad slides & backdoors

So this is one of the slides that Snowden gave us and it shows how, in this case the NSA thinks about this stuff. They have back doored most major IT-products. So, that's the stuff in your home, but also the stuff that you never see but you do depend on nonetheless, to get fresh milk for instance. If you work in IT you will know most of these brands, many other people will at least recognise some of them. It tells us that all these things have been back doored, by design, intentionally, and that makes spying a lot easier. So collecting information about the fact that you are all here now with your phones, listening to me, the NSA knows that now. If you are listening on YouTube, the NSA knows this now. Sorry. It also tells us that the NSA with the budget of a small nation, makes really bad slides. They need some help with that.



TOP SECRET//COMINT//X1

NSA Strategic Partnerships

Alliances with over 80 Major Global Corporations Supporting both Missions

- Telecommunications & Network Service Providers
- Network Infrastructure
- Hardware Platforms Desktops/Servers
- Operating Systems
- Applications Software
- Security Hardware & Software
- System Integrators

EDS
AT&T
Qwest
H-P
Motorola
CISCO
Qualcomm
Oracle
IBM
Intel
Microsoft
Verizon

TOP SECRET//COMINT//X1

Digital weapons lost

But it gets worse. The NSA also makes digital weapons to attack the very systems we do try to secure and then it loses those weapons and other people may abuse them. This happened a couple of years ago when somebody turned one of these things into a weapon and took down 40 hospitals in the UK, amongst other things. That was in May 2017. A month later another computer virus, also based on this lost weapons toolkit took out, among other things, a container capacity in Rotterdam Harbour. This is one of the biggest harbours on this side of the planet. And that meant no new car parts, no new clothing and no feed stocks for those cows that make the milk for you. This brings us the stuff that we need to survive. So the NSA's wish in this case to spy on the world, apparently mostly for economical en political reasons, has made us all a lot less safe. This is a very big problem.

Zero effect on terrorists

Regrettably none of all this spying has done the thing it was supposed to do, which is: prevent terrorist incidents. Zero effect. This is researched by both the US Congress and several other academic institutions. So, it is not doing what it is supposed to do, it is just causing lots of other problems. Despite all of this being ‘out’ – it has been in many newspapers for a couple of years now, it is no longer a secret, everybody knows – this does not mean that it stops. In fact, the recent US government has sort of doubled down on the policy of ‘collect everything’ and we will sort it out later. In order to collect everything, we need everything to be insecure. The fact that then we are all insecure, that’s just bad luck for us.

Encryption and open source

Also thanks to Snowden, we know what does work. That gives us the path forward to get out of this big mess. There is light at the end of the tunnel and that is what we need to work on. We know it works:

- we need strong crypto systems, and
- we need new kinds of computers that are built in Europe, for us and ideally by us – as close as possible to us – on the open source philosophy, whether the computer you own that is in your home, or the one

in the hospital you visit, which is accountable to you as an end-user. Not to some American company and/or the NSA.

New is easy

It may seem like a big task to start using a completely new computer that today does not even exist yet and that you've never seen and that you've never used, but I am absolutely certain that all of you can use, learn to use this new computer. That is because you all have a smartphone and they did not exist 10 years ago. You are all using those and nobody got a special course in it. So it is completely obvious that you can all learn to use a new computer that did not exist 10 years ago, because you already did it. Never underestimate your ability to learn new things when it comes to things like computers or many other areas.

Open standards work

Some people might say that it won't work with all the other stuff, if you have all these new computers that are different from the other ones. I call BS on that and my proof is the internet. The internet is billions of computers, produced by tens of thousands of different companies and it all works together. Why? Because of open standards, because of a common language that makes everything talk to each other even if different parties make it. For the techies... I know the internet does not really look like this, but let's keep that between us.

Before or after?

If there are lots of fires, of course we should buy lots of fire trucks. It is great if fire trucks come screeching down the road if there is a fire, but that is after the fact. This is what many security products like virus scanners and other things do: it is solving the problem when it is already exploding in your face. If the problem is that there are a lot of fires, maybe teach people not to smoke in bed, or other forms of knowledge and behavioural change that allows us to make slightly other choices and not get into trouble. Referring to the presented slide with Marilyn Monroe smoking in bed: “Marilyn, please don’t smoke in bed.”

I have deep faith in the idea that knowledge is power and that knowledge empowers people. That is why I teach digital self-defence. It is not about the boxes and the technology products, it is about the knowledge that people have in their heads and that they share with others that allows them to protect themselves and protect people around them.

Contribute

Everybody can contribute to this problem. And we are going to need everybody. If you are a software engineer, amazing, you can work on making the software better. If you are a graphics designer, you can make it maybe more shiny and more beautiful. If you are a linguist, help translate documents, if you are a writer you can maybe make them better. If you are a marketer, we need to make this desirable for people, even sexy, hopefully. If you are a teacher, we are going to need a lot of teachers. Everybody can contribute a little to this problem. It may seem that taking on the spying powers of global superpowers is a very daunting task. However, you should never shy away from daunting tasks, that's what really makes things worthwhile to do.

I have full faith that we can do this and I invite you to be part of that solution. We can do this, together.

2.

Ask your government why (and they'd better have good answers)

AUGUST 17, 2017 –
ARJEN'S PLEA AT THE PRESS CONFERENCE
'AUSTRIA UNDER WAY TO A SURVEILLANCE STATE'
(WITH NSA WHISTLEBLOWER BILL BINNEY)

"Mass surveillance does nothing to increase security while the new mountains of data create security risk themselves" ~ Arjen Kamphuis

My name is Arjen Kamphuis. I work on information security, which used to be specialised somewhere in a corner of an IT department somewhere. These days it's about fundamental human rights, things like privacy, the ability to journalists to protect their sources and in economic terms it is also about countering industrial espionage, which costs Europe something like 250 BLN euros per year.

Mass surveillance is wrong

Mass surveillance is wrong in many legal and moral terms. It is against the principles of democracy; it is against the United Nation's declaration for human rights and many other basic legal frameworks that we have. However, if such principles do not move you, maybe we can simply point out that it does not work. You can pick either one of those and those should be two good reasons to not do it.

Measures that don't work

However, the government - not just this government but also those of other countries in Europe and elsewhere - keep proposing these things. For instance after the Paris attack in late 2015, before the blood on the sidewalk was even dry, politicians were screaming that we now needed to ban all forms of encrypted communications between citizens. The funny thing was that encrypted communication played no role whatsoever in the preparation to these attacks. In fact, the attackers were all individually known, many had posted their weapons training in Syria on their Facebook page. They were all using phones that were running on their own name. They were using their own credit cards to rent the cars to go to Paris.

Why, government, why?

So, the measures proposed after the event would have had no impact on the ability to prevent the event. And that backs the question to these governments: why are you proposing things that anybody with half a brain can figure out in 30 minutes, do not solve the problem. So, I think it is also to the citizens - of Austria in this case - to ask their governments: are you merely incompetent or is there some other agenda going on here. Because it is very clear that mass surveillance to preventing terrorism does not work and we have seen this in Europe repeatedly and again. So it is not even a discussion. It is also however a fact that mass surveillance is very suitable for repressing democratically legitimate activities in society, such as journalism.

Huge databases, insufficient protection

Another problem with mass surveillance is that your government will be creating giant new databases of the private lives of the citizens, while their job is to serve them. Then the question is: can they protect those data mountains? Any government that thinks they can protect such data mountain, I would like to remind of the fact that the National Security Agency (NSA), the world largest intelligence agency with the budget the size of some smaller countries, was not able to prevent Edward Snowden walking out of the door with tens of thousands above top-secret documents. To this day they do not know exactly what he brought with him, so they need to consider all their documents compromised.

So, if the NSA cannot protect their database, do you think the Austrian government can protect a database about the lives of Austrian citizens from the 20 or 30 capable intelligence agencies in the world? Or dozens of advanced criminal organisations that might go after this data for purposes?

No, of course not. So the best way to prevent this is not to create a database in the first place. Particularly given the fact that it does not do anything good for the stated problem anyway. This, aside from the fact that it is going to cost a pile of money, which we could use for other stuff.

Backdoors and kill switches

We also know thanks to - well to Bill and even before Bill to Duncan Campbell, a British journalist who did good work - but we know since Snowden for absolute sure that all United States information technology products and services are backdoored by various intelligence agencies including NSA and CIA. The kill switches in those products are actively being used to be able to switch of countries. That is not just countries like Iran or maybe North Korea, but it is also countries like Austria. All modern countries using American information technologies are under an American kill switch. Everything in you society runs on chips, from the logistics in your supermarkets to the energy infrastructure, to hospitals, to everything your government does. If somebody foreign can switch that off (and yeah, it is now the orange king in Washington who controls the off-switch and he tends to have some impulse-control problems, so maybe this is worrisome), then it is not just him anymore because of course the secrets of these backdoors are out on WikiLeaks and are now in the hands of dozens of other parties, including again criminal organisations who can now switch of countries at will if they so desire. Usually they do not desire it because it is better to thieve a country empty than to crash its economy.

We need another IT

Running on these kinds of technology is a big strategic risk to the physical and economic well-being of the Austrian citizens. So again, the question to the government should be four years after Snowden gave us the very clear and documented proof of these problems: why are we continuing to do this, why do we continue to spend 15 to 20 BLN euros of our money to buy foreign spyware that can destroy our society instead of using that to create 350,000 IT jobs in Austria and build our own technology and then we are in charge of our society as a sovereign democratic society should be. So there are some policy implications and again it is not for journalists to ask the finer technical details, but it is for journalists and for citizens to ask their government: why are you doing this, come up with a good answer. And then we are going to ask some follow-up questions as well. That would be good. If governments are all doing these things, you do not have to have all the answers, but you have to ask: why? And they better have some good answers or otherwise maybe do something differently or stop doing it.

Be a better journalist

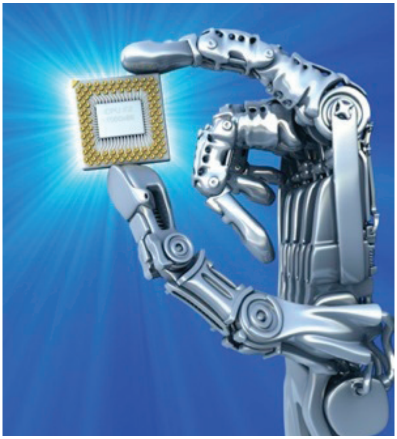
Lastly, information security is a big thing for journalists, or should be. If there are journalists in the room, in 2014 I wrote a book called 'Information security for investigative journalists'. It is easy to find on the internet. It is a free download and it is available in four languages. You can download it for free, you can spread it among your colleagues for free and there is many people across the Europe continent you can invite to get training from. They will often do it for merely a good meal or maybe they will charge a little bit for it. The technologies described in the book are being used by advanced investigative journalists across the world, by team WikiLeaks, by people like Edward Snowden to protect themselves and the people they work with. So we know from practise that they work against the most extreme surveillance regimes that exist in the world. We have made this book freely available and we have made this knowledge freely available and all the software we describe is also freely available to everybody. So please go and have a look at that and use it to protect your sources, your story and yourself and just be a better journalist.

Thank you.

3.

Future shock - What's it for? Understanding systems and policies

2009 - 2013



For over a million years we lived as hunter-gatherers in small family groups, for thousands of years we lived as farmers in small villages, for 200 years we lived in cities and built industry. Now we live globally in a world that is changing faster every day than ever before through new ideas and technologies.

Sickness and mortality?
Scarcity of material goods?
Humans as the most intelligent beings?
How very 20th century!

Old worldviews & new tech

Our history has not prepared us for these changes, our cultures, ideologies and religions provide no answers to many of the new questions we are faced with. Trying to impose old worldviews or ways of doing things on a new world is a recipe for failure, whether you are a company, government or individual.

For businesses, the challenge will be to provide valuable products in a world where many things that were expensive in the recent past, have quickly become very cheap or essentially free. Governments will struggle to remain relevant in a world that moves much faster than they can, and where geographical location is becoming less and less important for the individual citizens' identity, income and social network.

All of us will be challenged to rediscover what being human means in a world that is constantly changed by new technologies that we cannot really control. Do we try to stop these changes or can we adapt to them? What are some of the risks we face if we use all these new technologies? What are the rewards we might miss out on if we decide to not use them?

There are no simple answers but a greater awareness of what is on the horizon will allow us to find solutions that will make the future a lot better and interesting for all of us.

- Become aware of the radical new speed at wish the world is changing
- Learn to see the edges of your own thinking, then step over them
- Understand the fundamental impact on your profession and business

The future shock workshop will make you more aware of the depth and rate of change in the world and how it will affect you, your business and the expectations you have for the future. We look at the history of strategic change and see what we can learn from them. What worked in the past and why? Who should be involved in strategy development? What taboos prevent you from seeing clearly?

During Christmas 2000 I made the original version of a presentation to help people outside the technology field understand what the possible mid-to-longterm impact of tech really is. It was based on many of the online discussions I'd had over the previous four years. It deals with both familiar issues and thing often unknown outside a small circle of specialized researchers and thinkers. I expected it to be outdated within 18 months, but instead it is still a useful tool today to open people's minds to the possibility that our future may be very different from the fundamental rules we are used to. But why not judge for yourself?

Update 2013:

Exponential out of control

My central new insight to this topic is that exponential change does not only work 'up' (Moore's law, Kurzweil's law of accelerating returns) but also the other way: exponential out of control financial systems and military-industrial-security-complexes causing exponential depletion of critical resources. All of this is very bad but the exponential climate disaster is now rapidly approaching a level that could end up killing more people that all the wars ever (and perhaps all of us). Welcome to the age of consequences where 'crisis' will be the new normal.

Discuss the bad news

We really need to discuss some bad news about exponentially growing problems of resource scarcity, environmental degradation and the policy non-responses of our governments so far. A lot of activism against things like 'The War on Terror' or the various other ways our governments have lost their democratic ways, seem to be working from the assumption that most of the problems are just a misunderstanding. And if we can just explain the facts to these, not so smart, but essentially well-meaning people in Brussels and Washington everything will be OK.

This model of reality is good for being funded as an NGO and being invited to talk to aforementioned well-meaning people. It is not good for actually understanding and influencing what is going on (firstly because it ignores the fact that politicians in Brussels and Washington are really not in charge). Let us at least consider the idea that these ‘crazy’ policies are not crazy at all but are actually working perfectly. That is for the actual goals, just not the officially stated ones.[2]

Let’s talk. But let our talking be based on a harsh assessment of where we really are, not some politically convenient pretence of where we should be or would like to be.

4.

How the monkeys got to Mars

2010

Long ago, there were some monkeys on the African savannah. It was difficult for them as they hunted other animals that were stronger and faster. Other animals could digest the dry grass and live with little water. The monkeys could do none of these things.

Brains

You would think they would never survive, let alone go on to play an important role in the evolution of the Earth. That they did so is through a unique combination of two things that led to everything else: an opposable thumb and big brains.

Separately, each of these makes little difference. Dolphins have large brains and are certainly intelligent. But without hands to apply that intelligence, they cannot build complex civilisations. Chimpanzees have thumbs, but lack the brains to make hand axes and build terabit optical routers. So dolphins and chimpanzees are in our zoos instead of vice versa.

New solutions to new problems

Humankind dominates the planet by intelligence, not by running faster, breathing deeper or chewing through the hide of an elephant. Intelligence, the ability to create new solutions to new problems, is the key to all that we have and all that we are. First, we use the thighbone of an antelope as hand axes or javelins, and not long after (in evolutionary terms) we have the improved spear we call the ‘intercontinental ballistic missile’.

At the same time, people tend to associate intelligence with book learning and unworldly academics. “You need more than intelligence to make it in this world” is often said, as if charisma and emotional sensitivity come from the kidneys instead of the brains. When you say the word ‘intelligence’, think not of a crazed professor, but rather of the difference between humans and chimpanzees.

Fundamental changes by writing

Technology comes from intelligence and has a fundamental influence on who we are and how we live. Fire, agriculture, bronze, the wheel, the domestication of animals and irrigation systems fundamentally changed our position in respect to all other animals. But with writing came a technology that improved on our most valuable feature. For the first time it was possible to record knowledge outside our brains, and save it over long distances in time and geography. This had enormous implications for the scale at which we could organise and the speed with which we could develop new ideas by building on the ideas of others.

Knowledge deemed a threat

Around 1440, Johannes Gutenberg invented the modern printing press. The effects of this invention pulled Europe out of the middle ages and into the renaissance, the scientific/industrial revolution and on the path to democracy. Suddenly books were affordable for an emerging middle class. There were books about issues, history, politics, science, and culture. For the Vatican, this free dissemination of knowledge and ideas was a threat and it therefore hired troops to destroy all the printing presses across Europe. Fortunately the citizens objected and a few tough fights over the right to freedom of thought were the result. Currently, this fight is being repeated all over again by Scientology and the music and movie industry, with an equal lack of success.

Rapid developments

Now that knowledge could not only be written down and shared but also cheaply reproduced on a mass scale, our civilization developed rapidly. Science brought new technology and soon the smoke stacks of the industrial revolution existed throughout Europe and then the rest of the world.

Then things really accelerated. The complex societies existing over a century ago needed counting machines and from this came all the computers we use today. The logical next step was for these computers to talk to each other, so the researchers who used them could work smarter together. Forty years later, it is impossible to imagine our daily lives without the InterWeb. Now we all have a printing press with a global reach.

More acceleration

Access for all is the next step in the development of our civilization. It is a step that is as fundamental as ensuring everyone can read and write. It makes us smarter as we get more information, knowledge and ideas more quickly and cheaply and we have more people to share with. The Internet and cheap computers in everyone's pocket create as much change the printing

een VRIJ en OPEN internet is het FUNDAMENT van een gezonde INFORMATIE-MAATSCHAPPIJ
APEN missen de hersenen om TERABIT OPTICAL ROUTERS en VUISTBIJLEN te bouwen
it's not about the WORLD OF design, it's ABOUT THE DESIGN OF the world
je kunt CONCURREREN met gratis
INTERNET VOOR IEDEREEN
32 VISIES OP internet, technologie EN maatschappij
in welk BED werd u WAKKER?
eens kijken waar die eeuwenoude routekaart me de komende vijf maanden brengt
zorg dat je INTERESSANT bent
XS4ALL
meer internet

press 550 years ago. Only this time those changes will develop ten times as fast.

Supersmart

But it may be that the effects of networked computers obediently following Moore's law are more fundamental. As computers make us smarter or even smart, they can be used to make more sophisticated systems even faster, which will in turn create more sophisticated systems, etc...

If the difference between chimpanzees and us ensures that we walk on the moon and the chimps are our pets, what are the implications of a system (artificial intelligence or human-machine combo) that is fundamentally smarter than the smartest man who ever existed? And if that cleverness is deployed to always-smarter successors, a self-perpetuating process begins. This would reduce the entire information revolution of the past millennia to a very minor precursor of the real landslide that is about to happen.

How did the monkey get to Mars? By using his big brains, opposable thumbs and some technical tools. And the internet is one of the most important of those to come along in the last 500 years.

I contributed to the Dutch book by XS4All
about the history and future of the Internet.[3]

5.

Voting computer: The zombie that just won't die

2012

In July 2012, the VVD and D66 political parties (the Dutch equivalent of the Conservatives and LibDems in the UK) again proposed that the Netherlands should re-adopt electronic voting. Earlier this year the Dutch Association of Mayors also called for their reintroduction.[4] Don't you just love it when non-elected officials comment on and interfere with the electoral process? :-)

The basic problem

While the use of voting computers in the Netherlands has been banned for over four years, even for water board elections, there remains a fundamental misunderstanding of the basic problem with electronic voting.

For me the questions start with:

- What problems do these machines solve?
- What is so important that we would dare risk undetectable fraud and loss of voter-privacy?

Detectability of fraud

I can see none. In the Netherlands the process of voting should be understood and monitored by *any* citizen. It is all about detectability of fraud. Undetectable voting fraud with paper ballots if very difficult, as opposed to using software that most cannot understand or check.

While the many clumsy security problems – for example: ‘Nedap/ Groenendaal ES3B Voting Computer – a security analysis’[5] or ‘Breaking secrecy of the ballot with a radio scanner, video’[6] – or the absence of the source code of the software in the case of Nedap and SDU voting computers, are excellent talking points for the media and political agenda, these issues are not the core of the problem. And although the voting computer dossier at the Ministry of Home Affairs is now labelled with a bright fluorescent sticker: “Radioactive, do not touch!”, there is still a risk that local authorities or suppliers will continue to feel that voting by computer is best “if we can just iron out a few little bugs”.

The fundamental principles

The real objections are more fundamental and have little to do with security bugs or open source code. They are the fundamental principles underpinning our democracy, and they are threatened by the use of voting computers. In the many discussions on mailing lists and web forums it seems that people have lost sight of these principles.

Fraud? Ridiculous!

In the first year of operations of the We-don't-trust-voting-computers workgroup[7], there were many reassurances given by government and suppliers that we should not be so suspicious. The Netherlands is a great country after all, and the suggestion that anyone would commit fraud with something as fundamental as the election was considered ridiculous. Committing fraud was simply unthinkable and further discussion or justification not considered necessary. This attitude demonstrates a fundamental misunderstanding of the essence of democracy. That is not a question of trust but distrust of organised power.

Power corrupts

Through trial and error, we have learned over the past few thousand years that power corrupts, and absolute power can corrupt absolutely. An enlightened dictator can be an efficient form of government, but how do you ensure they remain enlightened once they have the power?

Complexity of democracy

To solve this problem we have evolved a complex system of temporary mandate (four years), with checks and balances as the need arises. You can only gain power if the majority of people have said that they really want you there, and even then, you will be closely monitored by 150 other people who are also only be allowed to do so because of the vote of thousands of fellow citizens. The system is far from perfect and is plagued by inertia and a focus on what is hot in the media, but we have yet to invent something better. This system makes it difficult to take important decisions publicly without authorisation. A king or president cannot simply on a whim ruin the country or violate the fundamental rights of citizens - unless those citizens and their representatives agree to it by inaction, but then they only have themselves to blame.

Trust?

The abuse of power cannot be solved by online publication of a voting computer's source code, because citizens cannot determine whether the published source code actually runs on the specific voting computers in their neighbourhood. Even more important is the fact that 99.99% of the population cannot audit the code. Inevitably, it still comes down to having confidence in a very small group of technical experts. And having to trust a very small group (any small group whatsoever!) is precisely what we no longer want. If we have small groups of technicians whom we trust, we might as well make up the parliament based on a sample of a research firm.

That saves a lot of time and paper and there is probably a great evening of TV programs that can be built around it.

Intervention

It has often been said that paper ballots can also be fraudulent, with elections in places like Zimbabwe cited as examples. The important aspect here is not the possibility of fraud but the possibility of detection when it happens. Large-scale, and therefore effective, fraud in a paper voting system is impossible to keep secret and that makes it possible to intervene when small groups try to exploit the system. In most cases, fraud with voting computers is impossible to prove afterwards. The records are erased and there are no ballot papers available for another recount.

Integrity of the process

This was proven painfully during a local election where the candidate council member was also the operator of the voting computer. In the polling station where he was present, he received an unlikely number of votes (higher than all other locations in the municipality combined). Yet the justice department was hard pressed to find actual evidence against this potential fraudster. Nor could the man ever prove his innocence. The result is therefore a situation where the integrity of the process itself is called into question, and thus the legitimacy of the ballot.

The distinction is thus the detectability of fraud, not the (im)possibility of it.

Accuracy

Even with electronic voting with a printed ballot (the so-called 'paper trail')[8] there can be doubts about the results. Applications for a recount of a paper trail is also an immediate political issue (against winners, losers). At what point do we initiate a paper recount? Which sample is good enough for the loser? How do we determine that there is reason to doubt the electronic result? Is there a basic assumption that the computer counts accurately? So there are inevitable administrative and political barriers to requesting a recount. This, combined with the fact that polling can provide the perception of a 'winning' coalition in the Netherlands, makes it attractive to manipulate voting computers. What is it worth to control the election of the 20th largest economy on the planet?

No problems with paper

Despite minor incidents with the paper system, the integrity of the Dutch paper voting process has never been the subject of discussion. And even the Interior Ministry and TNO had to admit, after some urging from external experts, that the previous generation of voting computers was not compatible (nor had it ever been compatible) with the Dutch electoral law.

Incompetence

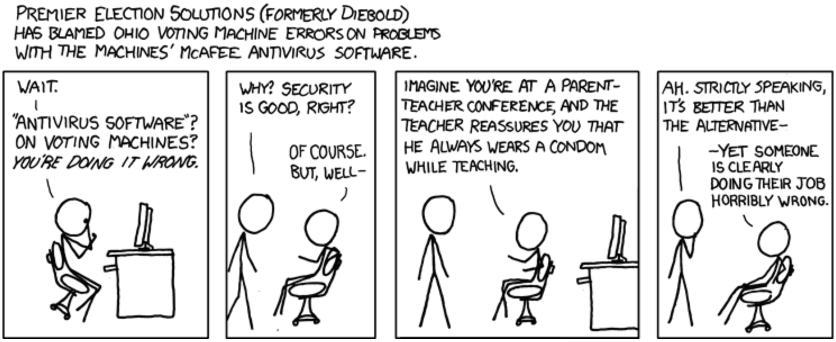
TNO hid the fact that the validation protocol of the integrity of the system had not been examined. Both the responsible officials and TNO's 'experts' were simply not competent to deal with this issue adequately. The OV-chip, EPD and the Diginotar dramas were repetitions of this incompetence, displaying no understanding, no adequate assessment frameworks, and no substantive oversight. And, of course, nobody is held responsible when things go wrong. After voting machines were banned, no civil servants and TNO employees were sacked for their screw up. Therefore there is very little confidence amongst external experts that future assessments on a different technical 'Solution' will be adequate.

Assurance of legitimate outcome

We must prevent a situation where the integrity of the electoral process itself can be questioned, and thus the legitimacy of the outcome. The vital distinction is the ability to detect fraud, not the (im)possibility thereof. Voting computers create serious problems, are more expensive that the use of paper, and they undermine the legitimacy of democratic governments. And as Churchill said: 'Democracy is the worst form of government, except for all those other forms that have been tried from time to time.'

I have always been very critical about the way electronic voting was implemented in The Netherlands. The lack of transparency of this method and the impossibility of recounts made this fundamentally incompatible with real democracy and, after some convincing by citizens, even the government agreed on this.

Original written for the website of 'Binnenlands Bestuur'.


PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD) HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.
WAIT.
"ANTIVIRUS SOFTWARE"? ON VOTING MACHINES? YOU'RE DOING IT WRONG.
WHY? SECURITY IS GOOD, RIGHT?
OF COURSE. BUT, WELL–
IMAGINE YOU'RE AT A PARENT-TEACHER CONFERENCE, AND THE TEACHER REASSURES YOU THAT HE ALWAYS WEARS A CONDOM WHILE TEACHING.
AH. STRICTLY SPEAKING, IT'S BETTER THAN THE ALTERNATIVE–
–YET SOMEONE IS CLEARLY DOING THEIR JOB HORRIBLY WRONG.

More about eVoting:

- https://www.researchgate.net/publication/301547849_E-voting_in_the_Netherlands_past_current_future
- https://english.kiesraad.nl/elections/publications/reports/2013/van-beek-committee-report/van-beek-committee-report/van-beek-committee-recommends-introduction-of-electronic-voting-and-vote-counting

6.

About Copyright

6.1 ACTA; war over. We win. Again.

2012

According to Dutch Economics Minister Maxime Verhagen, ‘ordinary’ people have nothing to fear from ACTA.[9] “This treaty is merely designed to shut down child pornography sites.” He really did say this!

Protecting copyright or children?

That’s good because, although I quite like a good download, I tend to limit myself to movies and books that fall a little more within the acceptable media spectrum. However, this statement gives us a fascinating glimpse into the mind of our Minister-of-All.

Apparently in the case of distribution of photographic evidence of actual child abuse, he is first and foremost concerned with possible copyright infringement. Is this a professional contortion or is he simply exceptionally goal orientated? This is what journalists should be pouncing on. For the lulz.

Copyright discussion

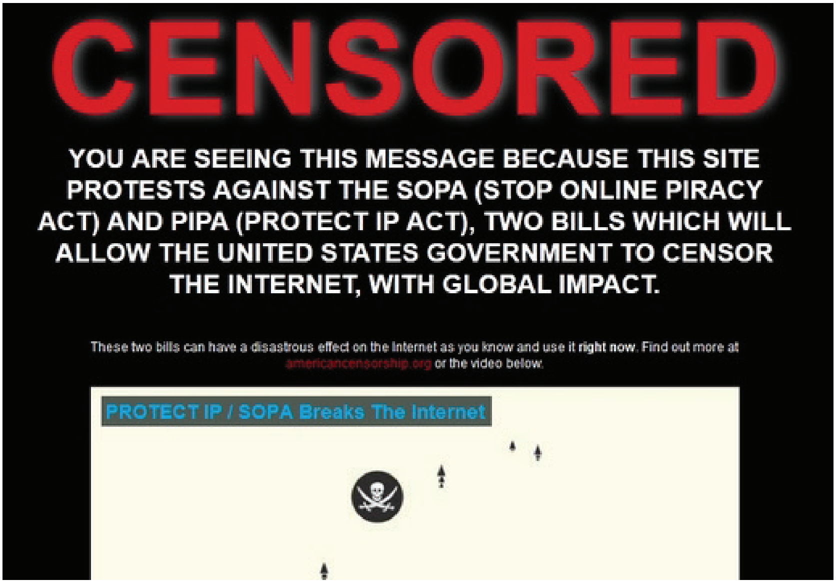
But beauty emerges even from the surrealist farce that is modern western copyright policy. No, I'm not talking about more music, movies or books, for there is no evidence that more culture is created by fanatically prosecuting 14-year olds for downloading. However, the recent weeks have clearly shown the usefulness of a common enemy. Thanks to ACTA, more Europeans than ever are involved in a critical discussion of modern copyright law and the balance with civil liberties. That is a wonderful development.

Furthermore, it now seems that ACTA is dying following the remarks of European Commissioner Viviane Reding (she senses the political climate). One European country after another is delaying signing the treaty. In the three years since the 'crisis' citizens have developed a fairly sharp bullshit filter to detect the kind of neo-liberal nonsense that ACTA is full of, and they will take no more. Like Software Patents it always takes a while for the protests to get going, but once they go representatives tend to choose the side of the people who can get them in a seat by voting in a few years.

Originally a Webwereld column

6.2 SOPA; not our problem

2012



CENSORED

YOU ARE SEEING THIS MESSAGE BECAUSE THIS SITE PROTESTS AGAINST THE SOPA (STOP ONLINE PIRACY ACT) AND PIPA (PROTECT IP ACT), TWO BILLS WHICH WILL ALLOW THE UNITED STATES GOVERNMENT TO CENSOR THE INTERNET, WITH GLOBAL IMPACT.

These two bills can have a disastrous effect on the Internet as you know and use it right now. Find out more at americancensorship.org or the video below.

On January 18 2012, was the big SOPA protest day. Wikipedia (in English), Boing Boing, Reddit and many other sites were blacked out. Other sites, and even Google.com had one-line banners beneath the bar exhorting me to contact the US Congress.

The link said: “Millions of Americans Oppose PIPA and SOPA because these bills would censor the Internet and slow economic growth in the US”.

Even a classic song[10] urges me “to call my congressman”.

American problem?

However, Google.nl, did not show this - clearly indicating that it perceived the matter to be an internal American political problem. In recent weeks however, there have been many calls for action outside the US against SOPA.

These calls have been synchronised with outrage and protests as Bush-Obama signed the NDAA anti-terrorism law. Under this law, anyone in the US 'suspected' of involvement in 'terrorism' (both nebulously defined) can be indefinitely imprisoned or even killed without trial or any other form of judicial review (think Stalin '30).

The anger itself is justified, but more than ten years too late. Indeed the only new provision in the NDAA is that the US can now treat its own citizens in ways that have been enforced against the world's other 6.5 billion people since 2001.

Originally a Dutch Webwereld column

6.3 The Declaration of Independence of Internet

2012

Original from 1776.[11]
Original from 1581 that is the inspiration[12] *for the original from 1776 here.*[13]

When in the course of human events it becomes necessary for people to dissolve the commercial, legal and moral bands which have connected them with an industry and to assume among the powers of the earth, the separate and equal station to which their most fundamental principles entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation.

We hold these truths to be self-evident, that all lives are enriched by the sharing of culture, that citizens are endowed by their democracies with certain unalienable rights, that among these are knowledge, true ownership of their property and the sharing of culture. That to secure these rights, laws are instituted among the people, deriving their just powers from the consent of the governed. That whenever any of these laws become destructive of these ends, it is the right of the people to alter or to abolish them, and to institute new laws, laying their foundations on such principles and organizing their powers in such form, as to them shall seem most likely to effect their safety and happiness.

Prudence, indeed, will dictate that laws long established should not be changed for light and transient causes; and accordingly all experience hath shewn that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same object, evinces a design to reduce them under absolute despotism, it is their right, it is their duty, to throw off such laws, and to provide new guards for their future cultural wealth. Such has been the patient sufferance of the people of the Internet; and such is now the necessity that constrains them to alter their former systems of cultural distribution. The history of the present copyright industry is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute tyranny over the culture of the people of Earth. These are just some of the effects of the lobbying of the copyright-industry.

The destruction of our cultural heritage by forced obliteration and decay, by forbidding or hindering the reduplication and sometimes even the restoration of cultural artifacts. - The destruction of our future, by frustrating education and the sharing of knowledge, thereby condemning many to lower life standards than they could otherwise achieve, especially in developing countries. - The destruction of the creative process, by legally forcing artists and authors to steer clear of any sources of inspiration, and punishing them for accidental similarities and citations. - The destruction of free access to key, contentious pieces of political information by preventing maximum distribution of this information. - The destruction of human and natural resources, by forcing the re-creation of works that would be perfectly usable with some minor rework, but not allowing such re-use. - The destruction of social and economic order, by allowing the control of much of our heritage to end up in just a few hands. Leading to a society where a few have a lot, and a lot have little. - The destruction of innocent lives by transporting citizens of other nations beyond Seas to be tried for offences that are not even offences in their home nations...

In every stage of these oppressions, we have petitioned for redress in the most humble terms: Our repeated petitions have been answered only by repeated injury. Corporations, whose character is thus marked by every act that may define tyrants, are unfit to be conduit of culture for a free people. Nor have we been wanting in attentions to our corporate cultural overlords. We have warned them from time to time of attempts by their lobbying to extend an unwarrantable jurisdiction over us. We have reminded them of the limits of our patience and the growing existence of alternatives to their wares. The most recent efforts of the copyright industry to circumvent our most fundamental democratic institutions leaves us no choice but to defend our culture by taking it out of the hands of these corporations.

We, therefore, the Pirates of the World, do, in the name, and by authority of the good people of the Internet, solemnly publish and declare, that we are free and united, and no longer recognise the legal or moral validity of the copyright claims of aforementioned corporations, that we are absolved from all legal and moral allegiance to these corporations, and that all connections between the people of the Internet and the copyright industry is and ought to be totally dissolved; and that as free and Independent people, we have full power to download, distribute, remix, broadcast, perform and to do all other acts and things which Independent people may of right do. And for the support of this declaration, with a firm reliance on strong crypto-logical protection, we mutually pledge to each other our lives, our fortunes, and our sacred bandwidth.

Originally a Webwereld column

6.4 Internet, Privacy, Copyright; choose two

2011

The Dutch Considerati think tank reported[14] earlier this week that there is still widespread downloading in the Netherlands.

Scope

Nevertheless, for an allegedly ‘broad’ piece of research, some key parties were missing - Bits of Freedom, for example. The study also did not consider fundamental questions about the social or economic value of copyright that lasts for more than a century (when once, it only lasted for 15 years), probably because those ordering the report did not want that question asked, let alone answered.

There was also no mention of the copyright industry aggressively lobbying[15] behind closed doors where laws are hammered out that our European representatives are not even allowed to see, let alone influence (read my article ‘Game over’).

Reduced to finance

The entire debate is reduced to a financial accounting exercise for a particular industry. So all is perfectly OK then, as I have nothing to do with it – I do not work in that industry – nor indeed do the vast majority of people. The comments on the website of Webwereld.nl quickly show that almost nobody takes such research seriously.

What blocks what?

A lawyer from the American RIAA recently added some colour by saying that the public domain blocked free market capitalism.[16] So much honesty can be scary sometimes. But the recent high point of the 'e'-G8 meeting in Paris was when Sarkozy and a few captains-of-industry gathered to decide what we should be allowed to do with our internet in the future. In response, a few uninvited representatives of civil liberties organisations held their own press conference (check out the video in which Prof. Lawrence Lessig sums it up nicely from 7:00 minutes onwards).[17]

Interests

These examples make it absolutely clear that the idea of any reasonable discussion with these vested interests is pure fiction. Wise people like Lessig[18] have been trying to start such a discussion for a decade, without success. Writer and activist Cory Doctorow[19] also tries to find a reasonable ‹middle ground› between the interests of authors, the copyright industry and the rest of society, and himself provides a good example with his DRM-free books. The copyright industry (or 'entertainment industry' in the Considerati report) ensures that any such a discussion is absolutely impossible by claiming industry interests and rights are absolute, without providing much of a broader social context. Large parts of the Considerati report read along the lines that providers of bottled mineral water are losing a lot of money because the local municipality washes its buses with tap water.

Human rights

This week, a UN report[20] declared that uninhibited access to the internet was a human right. This makes the French HAPODI law (whereby, after three alleged transgressions, the citizen is disconnected) a human rights violation. As long as people have internet access, they will download material. If there is anything to be learned from the internet›s last 15 years, it is that repressive measures against making digital copies always fail. Next year there will be yet more storage, wider bandwidths and cheaper processing power. This will only stop if we give up those basic rights as defined by the UN. A digital police state of Stalinist proportions would be needed to prevent copying. It is not insignificant that it is the copyright industry itself that is blocking any real move towards a wide-ranging public discussion on the reform of copyright.

Internet, Privacy, Copyright; Choose two

There is a well-known rule for complex projects: Good, Fast, Cheap - choose two. You can get good and fast, but it will cost. Good and cheap is possible, but it may require a little patience. All three at once is usually not possible. We can apply a similar formula to the ‘download debate’.

We can have the internet with the current functionality and openness while maintaining the right to privacy and free speech - but maintaining a 20th-century copyright model at the same time is impossible. Or we could give up our privacy and other civil rights to allow one specific industry to earn money in the same old way for a little longer. A last option would be to switch off the internet. That is not realistic: a country like the Netherlands could not survive a day without the internet, any more than it could survive without electricity.

The pain of choice

As a society we are going through the painful realisation that we can only have two out of the three options. Different vested-interest groups would no doubt make different choices but, like the vast majority of the people, I opt for the internet and privacy (this symbolises a whole range of civil rights). And thus the outcome of the process is already established, assuming we have a somewhat-functioning democracy (ACTA people do sometimes have doubts about this). Lawrence Lessig once joked during a presentation in Berlin that he, like Gorbachov, wanted to reform the system enough so it could be kept in place. Reform does not appear an option; rather a non-violent revolution is likely to happen.

Social change

Like any social change (the abolition of slavery, universal suffrage), this is also accompanied by heated debates, occasional legal sabre rattling and periodic propaganda reports from hired guns. But historically that will be just so much background noise. Maybe there will come a time, in the not too distant future, when basic civil rights make a comeback, upheld by the legislature and supported by the law enforcement agencies.

Upholding our rights

Until then, we citizens must defend our online rights with technical skills. Privacy can be upheld with crypto. To ensure mobile network neutrality, run all your traffic through a VPN. On a day-to-day basis it is not crazy to suggest that we should all explore the use of privacy tools more thoroughly.

Originally a Dutch Webwereld column

6.5 Close the Loop

2010

Now that The Pirate Bay is outlawed in the Netherlands - although this ban has yet to be tested in Dutch courts - the copyright industry and its tame lobbyists face a difficult choice: should they take their customers to court or not?

Lobby

This question is crucial to the survival of the lobby groups. Since the cost of fighting downloading is much higher than their income, large entertainment companies constantly need convincing that all these indirect lobby costs will at least produce results in the longer term. Nobody wants to think that the funding of lobby groups is ineffective, even if those organisations claim hundreds of site removals annually.[21]

Avoiding detection will be less hard

The entrenching of the battle lines is probably good for providers of innovative services, such as proxies that can run your internet traffic through other countries. There are also more complex and smarter things that experienced internet users can do to avoid detection. Like the process of downloading itself, these will become cheaper and more user-friendly in future, so that eventually everybody can use them.

Online control, offline sharing

Furthermore, any attempt to tighten online control will make offline sharing more attractive. With terabyte hard disks and 32-gigabyte micro SD-cards, the bandwidth in your pocket[22] is probably higher than a cable or DSL connection at this moment. Technically not much can be done to stop people sharing bits, and the odious behaviour[23] of the industry itself causes any moral objections to evaporate faster than the Greenland ice sheet.

Prosecution of individuals

Individuals are now threatened with prosecutions along the lines of the German model (with a 2000-euro fine). But how many of these cases can the already-overworked Prosecution Service realistically process in a year (thanks to other nonsensical bans on certain recreational pharmaceuticals)? Even making a grossly inflated estimate of 1000 prosecutions a month, those still only results in 24 million euros worth of fines *per annum* – and obviously, that is only if they win every case, which is highly unlikely.

Cultural solidarity

If the companies in the copyright industry actually take this step and go to legal war with their customers, it will not take long for someone to set up an online cultural solidarity fund. By becoming a contributor to that fund for a couple of euros per month, individuals can rely on specialist legal advice if they become one of the unfortunate 0.2-0.4% to be sued in any given year. With 1 million members contributing even 2 euros each month, you would quickly have a well-endowed war chest behind you, should you end up in court. Let us make the copyright lawyers work harder for their putative 24 million.

Resilience

As the case against Ziggo and XS4ALL demonstrated, copyright lawyers do not have nearly as much fun if their opponents fight back with a competent legal team. To gamble untold millions on legal costs to gain a paltry 24 million *per annum* is a risky strategy. Each lost case costs them money, and when you win, you gain more members (and thus a larger fund) to take to the next fight. Eventually it would be quite possible that any money remaining in such a fund could be used to create and promote culture.

These works would naturally be released under a Creative Commons licence. Of course, the "Bits-Of-Freedom-XS4ALL-Ziggo" Solidarity Fund for Culture and Creativity (just thinking out loud here!) would not allow the creation of more cultural works to be milked through classical copyright.

I'd pay

If such a fund existed to support cultural initiatives transparently and fairly, I would personally like to pay a bit more than 2 Euros per month (say 10 Euros). Especially when the *de facto* result is that I can make unlimited downloads - without having to worry that some copyright lawyers in the

Netherlands apparently do not know the difference between copyright infringement and theft (and yet are still employed as lawyers!).

Unlimited, risk-free digital culture for a tenner a month would be enough even for Maecenas - true wealth!

Originally a Dutch Webwereld column

6.6 Game Over

2010

Prof. Hugenholz's contribution to The Great Download Debate[24] in the Netherlands last week was clear: laws and treaties that are unalterable in the short term will determine the legal framework of the downloading debate. The professor himself called it a "legal reality check".

System lockdown

As I understand the situation, it does not matter much whether you vote for the Pirate Party or the conservatives in the upcoming election next week. Successful lobbying by the copyright industry over the last 100 years has led to a system of laws, treaties and international guidelines that has locked down the entire system, and which seemingly can only be changed when moving in the wrong direction. ACTA teaches us that the endlessly lengthening terms of copyright and the further privatisation of the investigations of alleged infringements are not a problem.

A no-win situation

So on the one hand our democracy is effectively sidelined. This apparently immutable situation gives the copyright industry a free hand to try to charge you every time you honour the works of your favourite artist by singing out loud in the shower.

Fortunately, on the other hand the vast majority of Dutch political parties understand that a serious enforcement of any download ban is just not feasible. Even hang-em and flog-em politician, Fred Teeven, will no longer be sending SWAT-teams to arrest 14-year-old girls who refuse to stop downloading. Even though it is technically possible to tap all the internet connections in the Netherlands, the political will is simply lacking. The electoral consequences would be almost as bad for the politicians as if they suddenly started promoting road tolls or scrapping mortgage tax relief. For most politicians it is a no-win situation, and they will not want to get their fingers burnt.

So as citizens, we have been completely sidelined in the ongoing development of these laws and treaties. However, as no one seriously wants to enforce them, it makes little difference in practice.

Laws of nature

Finally there is the technology that - fortunately - has its own laws. For example, the doubling of computing and storage capacity in a fixed period.[25] This has been a stable reality for many decades, independent of economic or geopolitical developments, and thus we can confidently predict it will continue into the future.

The technological capabilities of today and the very near future ensure that the laws and treaties referred to by Prof. Hugenholz will be unenforceable, even should the political will magically emerge. Every debate also underestimates the effective bandwidth of a backpack full of hard disks. Storage has become so cheap that is easy to give as birthday presents to your friends and family a year's worth of music on a hard disk or e-books on a micro-SD. And in about 14 months that will have doubled again.

Fast adoption of new tech

In other countries it may be possible to take draconian measures against less technically savvy people and scare them for a month or so, but then a next-generation technology, made sufficiently user-friendly, will be widely adopted by these people and their friends and family. In addition, the more draconian the measures, the faster the new countermeasures will be developed and applied. Many of the newer tools such as VPN tunnels and other privacy-enhancing technologies are not yet user-friendly enough for the mainstream, but that was also initially true of MP3 downloads. Today, even my father can rip a CD in minutes, upload the resulting files to his network drive and play them through XBMC (now Kodi[26]) on a variety of devices around the house.

Copyright industry lost

The download debate is over. The citizens have won. Not within the context of the debate, but by simply ignoring such obviously unreasonable laws and using technical capabilities of which the government is largely ignorant. Similarly in the 1990s the political debate and "policy development" around rapidly maturing biotech in plants was irrelevant before it had even begun, due to the pace of technological change and fast adoption.

It is this last point that our MPs and civil servants in The Hague should really pay attention to. We will revisit the whole debate again over the next 15 years, with the emergence of the 3D printer.[27] Just ignore it, while you print yourself a Kalashnikov (search online for 'ak47+blueprints').

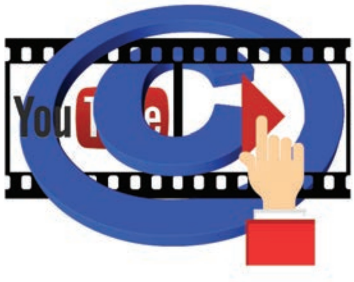
Originally a Dutch Webwereld column

Cory Doctorow wrote a piece[28] in the UK Digital Economy Bill and there is the usual discussion going on. Informative for those new to the debate.

6.7 A reasonable discussion

2010

In recent weeks a number of leaked documents has made it crystal clear how a cluster of companies (hereafter referred to as the ‘copyright industry’) warns off any threat to its commercial interests.



Money, money, money

The copyright industry consists of all those companies whose business models are based on the most extreme neo-liberal interpretation of copyright. In this interpretation, the ability to make money by endlessly re-selling the same piece of intellectual property is considered more important not only than democratic control over the creation of laws, but also than basic civil rights such as the principle of innocent until proven guilty.

Longterm copyright, less creativity

Where copyright once began in the 18th century with a period of 14 years, in the 19th and 20th centuries it extended to 70 years after the date of death of the author. It is not entirely clear how copyright 70 years after the death of a creative person can encourage more creativity (the original purpose of copyright).

There is no evidence that more culture is created by endless renewal and reinforcement of copyright; indeed, there are many indications[29] that it actively blocks both new creativity and the preservation of existing culture.

Commercial interests first, social later

First there are the now infamous Anti-Counterfeiting Trade Agreement negotiations. ACTA is an international treaty designed to combat the counterfeiting of branded products and other forms of copyright infringement. Although citizens of participating countries must adhere to this treaty on pain of subsequent fines or worse, they had no say in or even oversight of the treaty's creation. Companies from the copyright industry appear to have had a free hand in developing the content of ACTA. Citizens and their elected representatives were excluded and nobody will say why. That hardly creates trust.

Open source a threat for profit (to some)

Now, in a report[30] to the US government, it appears that the overarching pro-copyright lobbying organisation IIPA, the International Intellectual Property Association, wants to place a number of countries on a special watch list, because the governments of these countries actively promote the use of open source software. The deployment of open source is apparently comparable to copyright infringement, protectionism and terrorism, because it threatens the ability of proprietary software companies to make money. The logic of this is so distorted that you have to read it three times to believe that someone in his/her mind could write this in 2010. How nice that a Dutch caretaker government promoting open source can simultaneously be in the 'coalition of the willing' and the 'axis of evil'.

Reasonable consensus

The whole course of events raises the question of whether we, as citizens, can still have any rational discussion with these interest groups in the hope of reaching a reasonable consensus. A workable balance between different interests requires that both parties follow certain basic rules e.g. to respect the democratic state.

If, as in this case, lobby groups are so crude as to operate outside the normal frameworks, they leave the other party in the debate no choice but to do the same. That other party is we, the citizens, and we are many. And because we are many, we can innovate more quickly to circumvent any technical or legal barrier. In every public debate on copyright, the burden of proof is always put on citizens who believe that things should be a little less extreme.

Social utility of copyright

The copyright industry and its lobbyists have never been to able demonstrate the social utility of the endless tightening of copyright. An industry that desires legal protection for it's businessmodel, is it not reasonable that it shows society that this protection is of value to society? And if it will not or cannot… why should citizens give credence to the industry and its unilaterally-asserted 'rights'?

Democratic channels

The copyright industry seems headed for a total war against its own clients, with centuries-old civil rights simply set aside in secret negotiations. Obviously honest citizens will first try to change unreasonable laws through the usual democratic channels.

However, if these paths are obviously and actively blocked, then they will fall back to civil disobedience. If that does not help, strong measures may follow.[31] Fortunately in this case civil disobedience is extremely fun to do; download, upload, copy, share, crack, jailbreak and remix, until to all members of the IIPA either wake up to new realities or go bankrupt. And then we hold a huge party. With great music of course.

6.8 Debate between HAR and Brein

2009

On the second day of HAR2009,[32] a copyright debate was held between the entertainment industry and the hacker community at HAR2009 in the Netherlands.

Two views on copyright

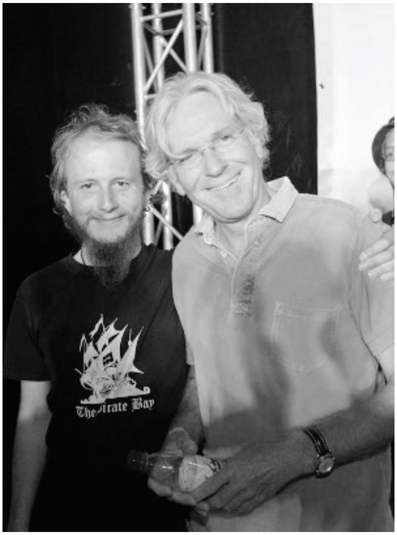
Tim Kuijk very bravely represented the views of the entertainment industry, while Walter van Holst and myself put forth a range of contrarian views and Prof.dr. Wilfred Dolfsma[33] moderated us and a full Monty Hall of hackers.

Because of some slight historic animosity between hackers and the entertainment industry we made a real effort to keep everything civilised. Since no tomatoes were see flying or Godwin's law invocations were required, I think we succeeded. I've stated my personal views on copyright in the 21st century on various occasions, for example read 'Internet, Privacy Copyright; choose two'.

Interest of society

Tim advocated the position that individual authors need to have the right to control what they create. Walter and myself argued for a more balanced approach given the inequalities between large media corporations, individual artists and the interest of society as a whole.

New culture is after all mainly built on what came before and so what came before needs to be re-usable. Disney made a killing by producing animated movie versions from European 17th century stories. But if it were up to the entertainment industry, copyright would last pretty much forever and so no new Disneys could ever come into existance.



Changes in distribution and sharing

Most people with knowledge of network technologies agree that the change in the way we distribute and share culture has already happened and organisations like BREIN are merely fighting a rear-guard action to delay the inevitable.

We can help the inevitable a bit by behaving like active citizens instead of acting like passive consumers. If you have to wait 5 minutes for that TV-episode to download you might as well write a courteous e-mail to your representative in parliament pointing out some of the fallacies in the copyright claims of the entertainment industry.

If we all do that then we'll soon see a repeat of the exchange between a US Colonel and his Vietnamese opponent in 1974: "You know, you never beat us on the battlefield." said Col. Summers and Col. Tu responded; "That may be so, but it is also irrelevant."

No criminals

In the second part the debate was opened up to the public and Anakata (one of the admin's from The Piratebay) stepped up to the mic to ask Tim not to call them criminals. According to Tim he never did. We will let the Swedish judge decide. After the debate Tim and Anakata demonstrated they could be friendly to each other in spite of the law-suits and counter-law suits flying through Europe.

With thanks to Reinoud van Leeuwen for the great photography.

6.9 Hamburg Declaration, newspapers can't network

2009

Last month, a group of European news outlets drew up the 'Hamburg Declaration'[34]. It demands that the European authorities take measures to prevent the re-use (they call it theft) of 'their' content. They want to demand money for 'their' news, as they get with printed editions.

To subscribe or not subscribe

Of course, publishers are free to hide their articles and other content behind a wall, available only to subscribers. They can also prevent search engines from indexing (and saving) their content. They can even choose to have no website at all, and reach only a shrinking and aging audience. You do not have to be a Twitter-using iPhone owner to predict what happens to a news organisation that starts a subscriber-only website or exists completely offline. For the growing number of readers of online news does not focus on individual outlets and there are many, many others which are eager to feed for free this readership's insatiable hunger for information 24/7.

Unsustainable model

The publishers claim that their model is unsustainable if they unable to pay editors to maintain standards, and thus their role as the watchdog of democracy is at stake. This thesis contains two parts, both doubtful.

1. The need for a classic, paid editorial as the only possible way to make news and information accessible. Very touching in a month where the traditional media are dependent on the Twitter- and YouTube-savvy citizens in Iran. CNN calls on its viewers every 30 minutes to continue sending in videos (with some interesting results). Nowadays on most newspaper forums, the comments and links posted by readers are often more relevant than the content of the article, which is just a copy/paste of AP or Reuters, and I had those already (RSS). Once the subject matter is specialised (and that often occurs in a complex world), the editors may not have the in-depth knowledge to understand an issue, so it is better to go to a specialised site where the authors as well as the responding readers are professionals.

2. The crucial role of the traditional media as a watchdog of democracy. Where shall I begin, in an area so rich with juicy examples? The New York Times that, after more than a year, admits[35] that it failed in just this role in the run-up to the attack on Iraq? The Dutch national news hour and so-called 'quality newspaper', which accused Iran of having a nuclear weapons program, while both the CIA and experts such as the International Atomic Energy Agency[36] are confident that this is not the case? The constant failure to ask the truly painful questions, as they might prevent editors from being 'granted' the occasional

> scoop? Bloggers who report[37] things that should be in the national news? Or how about Mr Broertjes, editor of The Volkskrant, who talked about a reducing investigative journalism because it meant taking people "out of production"? 'Production' in this context means reading the AP/AP or Reuters newsfeeds and other news releases, then quickly writing a short article. Exactly the behaviour newspapers accuse bloggers of.

Journalistst, guardians of democracy

Based on my experience of the established media in recent years, I just do not trust them as a primary source of information about interesting events; too often they have failed to ask the difficult questions. And whether that is down to incompetence, lack of courage or something else does not matter much. In a Europe where surveillance and censorship have become normal and where we get dragged into wars and occupations, there is plenty for the guardians of democracy to do.

So if the former watchdogs take up that role again, I will pay for a subscription, provided I get the information in a way that suits my lifestyle (and not once every 24 hours on a piece of dead tree). From the former office of Mr Broertjes, I hope the editorial staff find both courage and a spine.

6.10 Copyright destroying our culture

2008

In an article in the Dutch newspaper NRC on April 17th 2008, Martin Bossenbroek and Hans Jansen explain why copyright prevents the development of a national digital library. For such a library to work over the internet, existing law requires that all authors are tracked down and their consent obtained. In many cases, this is almost completely impossible.

The authors cite a specific example of a copy of the Dutch magazine ‘Panorama’ from 1921, to which dozens of freelancers had contributed. To trace all these people, to find out whether they died before or after 1937 (copyright is valid until 70 years after the death of the author) and then find all possible heirs is a mountain of administrative work that means it is impossible to make Panorama available online.

Only on paper

The end result is that the copy of the Panorama is preserved in paper format, and no one can use it for research or education on the recent history of the Netherlands. The actual availability of information for the community is effectively reduced to zero. It is even worse with rare nitrate films that will fall apart in a few decades and that, for fear of copyright, no one dares to digitise. Lost forever.

And that is crazy.

Human spirit for society

For the purpose of copyright law is ultimately to stimulate the creation and dissemination of works of the human spirit for society (and not, like the collecting agencies of this world would have us believe, to give publishers the right to print money). The question boils down to whether society actually benefits from copyright extending until 70 years after the death of the author. The view of financial reward after death will hardly encourage the author to create new work. In practice, moreover, even 100 years ago the greatest returns came in the first few years after initial publication; more so in today's faster economy.

15 years protection is best

Research[38] from Cambridge University last year shows that a protection period of 15 years provides the economic optimum balance between the financial interests of authors and the benefits of free availability to society as a whole.

Music and film industry = copyright industry

Copyright is a government-created artificial scarcity with one goal. However, in this century that original goal is clearly not served by laws that were made for it. Why is copyright so long? Lawrence Lessig has written extensively about this (book[39] - download[40]), but in short it comes down to ordinary lobbying by publishers and the music and film industry (I've always found it telling that it calls itself an industry - a name reflecting, without shame, its lack of beauty and creativity). Since the creation of copyright in the 18th century (mainly because of the invention of the printing press), the length of copyright has incrementally extended from the original 14 years to 70-years-after-the-death-of-the-author.

Cultural heritage at risk

With the advent of institutions like the World Intellectual Property Organisation (WIPO), this particular American model has been imposed worldwide. To become members of the WTO and thereby enjoy low import tariffs in Western countries, governments are forced to sign the WIPO treaty and are then saddled with copyright that puts at risk the reuse of their cultural heritage. Perhaps it is time that the Netherlands once again takes the lead in the dissemination of intellectual works, just as we did in the 18th Century. At that time inflammatory books were printed here that partly brought about the French Revolution (statements about cake also played a role).

Fundamental review of copyright

The availability of knowledge and culture to society is clearly not being served by current legislation. The solution is not a more complex system of exemptions, as Ewoud Sanders stated in his response to the NRC article, but a fundamental review of the purpose and effect of copyright. The research of Lawrence Lessig, the Free Culture movement and the recent research from Cambridge all provide good directions. Now we need a few policy makers with the courage to serve the community instead of the publishers and the music industry lobby.

This article, like all my public work, is under a Creative Commons License. After all, the greatest risk an author runs today is not that their work is "stolen", but is that it is not read. Share & enjoy!

7.

About government & IT

7.1 The other IT from another Europe

2014

Over the last 10-15 years public IT in Europe has not developed in line with public interests,[41] nor does it guarantee the fundamental rights of citizens such as privacy and freedom of expression. Tremendous opportunities in the field of economic development and employment have also been missed.

Paying (to be spied upon)

Europe effectively outsources much of its information processing (software & services) to foreign parties at the direct cost of hundreds of billions of Euros (typically around 1% of GNP). The opportunity-cost to local economic growth and employment opportunities are much greater than that. Even more costly than either of these is the de-facto handing over of control of data of governments, businesses and individual citizens to foreign spies who use it for political manipulation,[42] repression of citizens' freedoms and industrial espionage.[43] Although the warnings about the negative consequences of current policies date back at least 15 years, these aspects have been documented in irrefutable detail over the last year by the revelations of Edward Snowden. 12 months later, there has not even been the beginning of a policy response.[44]

It could all have been so different...

Another IT

In the first 21 months of the 21st century, the dot-com bubble burst and then three skyscrapers in New York collapsed. Between these two events, a largely forgotten report[45] to the European Parliament appeared in the summer of 2001. This report described the scale and impact of electronic espionage in Europe by the U.S. and its 'Echelon' partners (Canada, UK, Australia and New Zealand). Besides a detailed problem analysis, the report also gave concrete examples of IT policies that governments could take to significantly limit foreign intelligence spying on Europe.

In the same period was U.S. government won one of the largest anti-trust cases its history, against Microsoft,[46] and the EU followed this victory by launching a similar case that would also be won[47] leading to the highest fine to a company for economic crimes in the history of the EU.

It was against this background that thinking about strategic versus operational aspects of IT in the public sector changed. The report on Echelon made it clear that reducing IT into a merely operational exercise had disastrous consequences on the sovereignty of European states with respect to, in particular, the United States (and perhaps in the near future, China, other technically capable countries or non-state organisations). The economic consequences of industrial espionage against many high-tech and R&D-intensive companies became a major concern for the government. So...

From 2002 onwards, the IT policy of governments is be based first on the political principles of a democratic and sovereign state. This not only means a very different policy in the field of technology selection and procurement, but also in the balance between outsourcing versus in-house expertise and it requires an extreme degree of transparency from all suppliers. Open data standards for public information are required, and non-compliance results in severe penalties (although public ridicule from 2009 onward is generally the most effective). These new frameworks for public IT create a new market for service providers, who base solutions on so-called 'Free Software' (previously better known as 'open source'). The high degree of transparency both in project implementation as the technology itself make the norm for a well-functioning market and made recycling of (parts-of) systems. Spending on software falls sharply and the freed up budget is used for the recruitment of highly qualified IT workers under conditions that could compete with the offerings of market.

The full transparency with respect to both the IT projects and the tech itself, combined with a depth of expertise within the government, changes the market for public software and IT services. Quality rises steadily while prices remain permanently under pressure. Since all service providers have full access to all software used in government (with only a few exceptions in defence, justice and home affairs), there is a very open playing field where all providers are expendable (and those who perform below par are replaced regularly).

In addition, computer and IT education from kindergarten to university studies are fundamentally revised. Basic understanding of the operation of computers and information networks becomes as normal as reading and writing. From 2006, every fourteen-year-old is taught in school how to encrypt and what the disadvantages are of using software of which the source codes are not published.

Through this awareness among young people in Europe, the adoption of social media occurs very differently than in the U.S. Young people not only have end-user skills, but also real understanding about what is happening to their information when sending a message or upload a photo to websites. Being careful with your private information is considered cool. The social media landscape is not dominated by a handful of U.S. companies, instead there is a landscape of federated services such as Diaspora who compete among themselves, but are compatible in the same way as is the case with email. These services are sometimes somewhat centralised but, just as often, completely decentralised and run on micro-servers in many people's homes (such as the UK-invented 35 Euro RaspberryPi).[48]

Due to the high privacy and safety awareness, online crime[49] *does not have much grip on most European countries. Hardly anyone is naive enough to log on to strange domains or websites in response to a fake email that appears to come from their bank. In addition, the use of customised secure USB drives*[50] *created by various banks is accepted as obvious for any major online financial transactions. At the level of organisations, high levels of expertise and a high degree of diversity in technology implementations make for robust security that is only seldom breached. The large demand for experts in well-paid jobs also keeps many would-be criminals from selling their skills for more destructive applications.*

That is the IT that Europe could have had if other choices were made over the last 12 years. All the knowledge and technology for these choices were available in the first months of this century.

Social cost

Because these choices were not made, Europe has spent hundreds of billions on software licenses and services from American companies, while there were cheaper (often free), more flexible and safer alternatives available that would not operate as a foreign espionage platform. All these hundreds of billions were not invested in European service, training, education and R&D. The economic impact may be a multiple of the roughly $1 trillion in foreign software licenses spent by Europe this century, while the social cost resulting from manipulated politicians during transatlantic negotiations on trade or environmental matters will probably never be known.

Huge saving and improved safety, there is still time

Europe still has everything it needs to develop and implement such policies. It is not too late to turn, no matter how regrettable the policy failures of the last decade and no matter how many wasted billions. Today could be the first day of such a new course. Concrete examples in the Netherlands,[51] Germany,[52] France,[53] Spain,[54] the UK[55] and many other places show that this is not only possible, but almost immediately leads to huge savings, improved safety and independence from foreign parties in future IT choices.

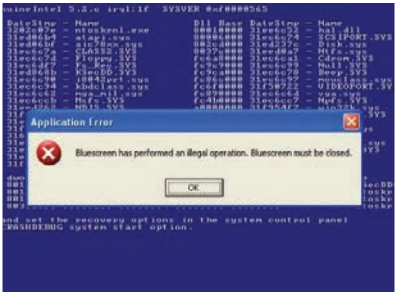
Political will

It is not often that regaining national sovereignty and the restoration of civil rights can spur national innovation and employment programs simultaneously. The only thing missing is the political will to stop rewarding businesses and governments that use their technological dominance to spy on the entire world. We have nothing to lose but our chains to the NSA.

Also on Consortium News and Huffington Post

7.2 IT and government, what to do?

2012



```
uineIntel 5.2.c irql:1f  SYSVER 0xf0000565

DateStmp - Name                   Dll Base DateStmp - Name
3202c07e - ntoskrnl.exe           80010000 31ee6c52 - hal.dll
31ed06b4 - atapi.sys              80006000 31ec6c74 - SCSIPORT.SYS
31ed06bf - aic78xx.sys            802cd000 31ed237c - Disk.sys
31ec6c7a - CLASS2.SYS             8037c000 31eed0a7 - Ntfs.sys
31ec6c7d - Floppy.SYS             fc6a8000 31ec6ca1 - Cdrom.SYS
31ec6df7 - Fs_Rec.SYS             fc9c9000 31ec6c99 - Null.SYS
31ed868b - KSecDD.SYS             fc9ca000 31ec6c78 - Beep.SYS
31ec6c90 - i8042prt.sys           fc86c000 31ec6c97 - mouclass.sys
31ec6c94 - kbdclass.sys           fc6f0000 31f50722 - VIDEOPORT.SY
31ec6c62 - mga_mil.sys            fc890000 31ec6c6d - vga.sys
31ec6ccb - Msfs.SYS               fc4b0000 31ec6cc7 - Npfs.SYS

and set the recovery options in the system control panel
CRASHDEBUG system start option.
```

Application Error

Bluescreen has performed an illegal operation. Bluescreen must be closed.

Recently, along with other 'experts', I attended a Parliamentary Working Group to answer questions about government IT projects. This was a Parliamentary group of MPs investigating the many IT failures of the government. After the summer (and the sept 12th elections), the investigation should begin with a sharp set of research questions. The invited experts were there to help formulate the right questions.

Unanimous

In my next article 'Parliamentary hearing on IT-projects, security & privacy', you will find to some of the available online advice written by the working group and the video stream (all in Dutch). It was striking how unanimous the message presented by all the IT experts was, given the variety of their backgrounds.

Like other columnists and opinion writers, I also emphasised the failings of government and egregious damage to national security, privacy and general public funds.[56] From available data, in terms of the government, the cost to the Dutch has moved from millions to billions of euros annually.

Constructive consultations

With such a government, it is like shooting fish in a barrel for columnists. Therefore, it was refreshing on this occasion to make a more constructive contribution. Although, it was a pity that meetings like this do not occur more frequently and are not better attended by the officials and suppliers who are responsible for all these projects. As 6 billion euros pour down the drain every year (and that is only the out-of-pocket costs - the social impact may be much higher), it might be a good idea to hold consultations more often. While I doubt that the gathering last week has any ready-made solutions for all the problems, I think there is a reasonable degree of consensus about their root causes:

1. Wrong incentives for both government and suppliers
2. Too little substantive knowledge
3. Total lack of oversight and transparency
4. Dangerously naive attitude to security risks
5. There is no discernible ambition to rectify any of the above points

1. Wrong incentives for both government and suppliers - Who actually has an interest in completing projects within the agreed period and under budget? Nobody. Not the supplier, who could just add many more billable hours and therefore finds added complexity much more lucrative. Not the responsible bureaucrats, because when a project runs, they have a job and a growing staff to do things - the larger your group, the more important you are. In addition, because projects quickly become a political matter, then a 1,000% overspend becomes perfectly acceptable in order to save the neck of some senior official. There are never any penalties for any of the involved parties, no matter what the scale and consequences of the failures. The same officials continue to hire the same 10 major suppliers.

2. Too little substantive knowledge - This allows suppliers to drive the process because most government departments lack the expertise they allow suppliers to drive virtually all substantive activities. This allows vendors to interfere in advisory roles about the delivery of products and the implementation of services. This is very profitable for the suppliers, but not so great for the cost or technology choices that are supposed to work in the interest of the government and the citizens.

3. Total lack of oversight and transparency - There is so little transparency that the government does not know what it has, what it buys and how much it costs. Previous attempts by parliament to get an insight into all this failed. The consequence is that most so-called 'business cases' are mostly hot air. If it is impossible to assess what something currently costs and the expense of replacing it, we are sailing blind. Probably on the 'advice' of the vendors mentioned in point 1.

4. Dangerously naive attitude to security risks - The recent incidents involving SCADA systems and many, many other broken online government services, show that the security risks are not incidental but structural in nature. Add Stuxnet to the mix and it is clear that public systems can easily be manipulated. The social consequences of a targeted attack are difficult to predict, and the government has no contingency plan whatsoever. It is not even clear who is responsible for picking up the pieces when certain services fail.

5. There is no discernible ambition to rectify any of the above points - The government remains quite content to define them as an immutable law of nature or fate and therefore outside its ability to influence.

That all sounds terrible. The question remains – is there anything we can do? Yes, *we*. Because if you have read this, you will probably be concerned about government, your hospital that you might need some day, the school where your children go, the pumping station that keeps your feet dry.

Ambition

The solution starts with recognizing the five points above. It is not good enough to dismiss the scale of the problem with statements like "but it is not always wrong..." A car which sometimes does not explode is not good enough. After recognising the problem, there must be a real will to improve (perhaps spurred on by a penalty imposed by parliament). The government must have the ambition to seriously revise its traditional 'modus operandi'.

In addition, there must be the will to have a real, effective government, not some call centre for a corporation. The government is not a business, so it should stop pretending. This goal should be the visible core of all subsequent behaviour. Greater transparency will sharply expose any lack of expertise and the wrong incentives; as a result, targeted action can be taken. Transparency also makes it much easier for other experts to advice government (for example about that naïve attitude to security).

How large, complex and important all these questions may seem to be. Yet, recently the more important questions were asked by Professor Eben Moglen in a masterly speech in Berlin: 'Why Freedom of Thought Requires Free Media and Why Free Media Requires Free Technology'.[57] Under the speech, there are now discussions that 'I Have a Dream'[58] meets 'Band of Brothers' (a vision combined with a call to action). That is how this speech should look to anyone involved in IT, and triply so to bureaucrats. I hope that our MPs can also spare an hour to watch it this summer.

To waste 6 billion Euros a year is bad, but to throw away the hard-won freedoms of the past 1000 years - that is really bad.

Originally a Webwereld column

7.3 Parliamentary hearing on IT-projects, security & privacy

2012

On June 1st 2012, the Dutch government's parliamentary working group on government IT-projects held a hearing of experts. Dutch journalist Brenno de Winter published his thoughts in 'HP de Tijd'. My written contribution below. Also read my article 'IT & government, what to do?'

Introduction - IT and the Dutch national government

Universality is an assumption of astrophysics that states that all phenomena, everywhere, behave as we observe them from Earth. I'm assuming that phenomena I have observed in specific government IT projects also occur in government IT projects that I have less information about (this is usually caused by the poor implementation of Freedom Of Information Acts, see the notes of Mr De Winter).

Accurate model

IT project management is currently based on a rather naïve model of reality: 'Smart entrepreneurs compete on a level playing field for the favours of the government, which then procures with insight and vision.' However, this model does not adequately predict the observed outcome of the projects. Whence this group.

Another model would be: ‘A corrupt swamp with the wrong incentives, populated by sharks and incompetent clowns’. This model has the advantage of perfectly predicting the observed outcomes.

The price of outsourcing everything

No vision, no vigour, no knowledge, and especially no ambition to do anything to improve on any of these. This is the overarching theme of all government IT projects I have experienced both on the inside and externally. And I believe it is the fundamental cause of the vast majority of practical problems the group wishes to understand.

Social problem becomes technical project

From Knowledgenet to the National EHR[59], the Whale project, voting computers, the public transport card, and the failed attempt to break the monopoly of large software vendors - NOiV[60]... the knee-jerk response remains the same: to reduce a social problem to a technical project that can then be quickly outsourced to IT suppliers and/or advisors. The societal aspects are quickly lost once the train of political promises, commercial interests and project logic leaves the station and becomes unstoppable.

Even the parliamentary group on IT projects aims to outsource part of its work to an external company. The chances are that the selected external company will already have as its main selling point an umbrella contract with the national government. Probably this company will already have been advisors on one or more of the projects that may be under investigation.

Attract competent personnel

In my experience as an advisor of a large government project (from the list of projects provided by the work group), I had to advise another consultant on how to hire yet other outside consultants to perform a security audit. The argument that the government has difficulty in hiring and retaining specialised expertise may be true in specific cases, but in reality, most of the hired 'IT workers' have no specialist expertise. Often they are generalists and/or project managers without substantive technical knowledge. The inability of government to attract competent personnel should be seen as a problem that needs to be solved, not as an immutable law of nature. If we truly want something to change, we really need to be willing to change anything/everything.

Scope

Focus of the research proposal: look at the forest, not at the trees. By focusing on individual projects it is likely that the working group will only look at operational issues within these projects. The broader, underlying causes remain hidden, yet that is precisely where many failures begin.

Moreover, it is especially important to look at such overarching issues as potential factors in future projects.

Lack of accountability

If anything has become clear since the Diginotar case, it is the total lack of accountability or sanctions subsequent to the failure of both executive and supervisory organisations and officials. Suppliers and officials who have endangered the security of citizens and the functioning of the state have largely remained in position, free to repeat their mistakes in a few more years. Evaluation, in this context, is therefore only useful if lessons learned from them, can be used to prevent a repetition of similar birth defects in new projects in the future.

Analyse context: causes and societal consequences of failure

When the senate cancelled the EHR project, there was great indignation about the 'wasted' 300 million Euros that had been spent. In my view, the 300 million is not the issue we should be focusing on.

If the figures used by the Health Ministry and Nictiz concerning the need for the EHR system were correct, the real costs of the failure of the EHR system over the past 12 years are more than 20,000 lives and 16 billion Euros. Therefore the real question is why Nictiz on the one hand did not have either the budget or the required mandate to deal with the problem, and on the other hand why this national disaster was not the most important issue for the Health Ministry to address. Why did the leadership of the Ministry not have its hand on the wheel, with weekly reports to the Cabinet and parliament?

If the publicly stated figures are incorrect, Parliament has been misinformed for more than 12 years and the project should never have been started. Both way, something went very wrong and it had very little to do with the technical aspects of the project (although there was enough to criticise there as well).

Transparency should be required

The above example is just one of many cases where the formal administrative motivation for a project and subsequently allocated funds and mandates, bear no logical relationship. In addition, the projects concerning the introduction of voting computers and the public transport card had logical holes of Alice-in-Wonderland-like proportions. A very high level of public transparency about new projects here, would probably have enabled citizens to provide both solicited and unsolicited assistance to the government in finding these holes.

It would also help to restore some confidence amongst citizens, whose faith has been repeatedly dented. On the one hand, the government uses its own incompetence as an excuse for failure, while on the other hand two weeks later, it will ask its citizens to rely on its ability to finish a new megalomaniac techno-fix for a complex social issue. The current deep lack of credibility ultimately becomes a question of legitimacy.

Selection criteria for examining IT projects:

- Extent to which the original official motivations and assumptions were not investigated or found not to be substantiated. What was the problem? How would the proposed IT project fix this? Why was the gap between policy and reality not foreseen?
- Social costs of not solving a problem (by the failure of the project); these are often multiples of the cost of the IT project itself.
- Damage to citizens and their rights because of the failure of project or because of incorrect technical and organisational choices made during implementation.

IT projects that the working group could include in the investigation:

- The EHR
- The public transport card
- The NOiV & the NCA investigation into the failure of this policy
- GOLD/DWR - introduction of the 'standardised' workplace for the national government between 2004 and today

7.4 Tech-politics and the importance of outreach

2012

In Cory Doctorow's column in the Guardian about tech-politics and the importance of outreach by the tech community, he makes the point that ensuring your rights through technical skills is great, but not much help to society if the tech is too difficult for most people to use. Outreach activities and the hard work of polishing technical tools for non-techie use are of vital importance. His column can be found here.[61] I think that one important aspect was missing from Cory's argument, so here is my additional comment on another vital aspect of current tech/internet politics to his article.

Broken politics

As nerd-politics is a subset of 'normal' politics, it is not just the nerd-part we need to worry about. The political system itself needs to function - at least some of the time - to get anywhere. If a country has a political system that retains the rituals of a democracy but no longer actually functions as such, then no amount of good nerd-politics (or politics of any other kind) will fix anything. Especially if such a fix threatens established and well-funded business interests.

It is perhaps no coincidence that all the bad tech-policy examples that Cory cites (SOPA, ACTA, TTP, DMCA, attacks on the Pirate Bay, mass reading of email, etc.) originate in the US and from there are foisted on other countries. While those countries deserve their fair share of blame for allowing a foreign power to bully them into this stuff, it is pretty clear where the problem lies. With or without nerds involved.

Ignore lobbyist' laws

Either we fix the completely broken US political system (and good luck with that!) or the rest of the world needs to get better at ignoring absurd US laws and treaties, cobbled together by lobbyists of private for-profit organisations. Neither those corporations nor general US politics concern themselves with the interests of the inhabitants of the rest of the planet. And the rest of the planet should respond accordingly.

Nerds (a.k.a. the tech community) can provide some tools to help out with that, as the Free Software movement and WikiLeaks have shown.

7.5 Waiting for the big one

2011

Diginotar's multiple IT failures in the public sector have been swept under the carpet. So far, nothing indicates that there will be any real change to the Dutch government's overdue IT projects. During the hearing in the Lower House, it was apparent that neither the government overseer OPTA nor auditor Price Waterhouse Coopers believe themselves at fault, despite the fact that as regulators they have rubberstamped the work of Diginotar for years. The decisions of the PwC auditors were obviously good because "they are executed by responsible professionals". This will be heartening for all those Iranian citizens who are suffering the consequences of this (think of an unpleasant convergence of kneecaps and power tools).

The unknown full horror

However, because of the chaos at Diginotar, we may never know for certain the full horror of those consequences. It is very simple for someone to take over an entire network and manipulate all the logs. The only thing we can really say with any certainty is that so far we have no reason to believe that IT security was any better in the past than the recently discovered FoxIT mess. The PwC audits are obviously not able to detect such a mess and OPTA apparently did not even look. Possibly Diginotar has been totally hacked for many years, and nobody noticed. A really smart spy or cybercriminal does his job and leaves no traces. The many detailed discussions about the exact scale and timeline of the hack have completely ignored this fact. From his grave, Socrates is smiling at the idea that we “only certainly know what we certainly do not know”.

Pertinent question

The most important question is surely: “How can we prevent such a critical part of our IT infrastructure from falling into foreign hands?” But this question was apparently not even on the radar of our regulators or MPs. Recent discussions about the USA browsing through our systems without judicial oversight, make this question particularly pertinent. Then again, perhaps I am somewhat naive to expect that my government to be both capable and motivated to protect the interests of its citizens.

Teamwork: it spreads the blame

Diginotar is yet another egregious example of a public IT function going terribly wrong at every conceivable level (selection, implementation, monitoring), and yet nobody being held responsible for the consequences. It is important to recognise that we shall probably never know how serious the real consequences were - especially for that unknown number of Iranian citizens. As a direct result, we must also recognise that we need to replace the people who did this ‘monitoring’ and the ‘methods’ they used.

To continue doing the same and yet expect different results is one of the definitions of insanity.

Know nothing, do nothing

If a key IT organisation appointed by the government fails, it is down to a lack of crucial expertise in the government. Everything is privatised and the resulting lack of expertise is an unfortunate consequence of a principle of degraded policy-making. Instead of identifying and solving this lack of substantive expertise, it is dismissed as an immutable law of nature. “It just is” that the government has no employees who have relevant expertise to evaluate, manage and oversee IT projects (or evaluate and oversee the hired vendors). Simultaneously, our citizens trust that same government to properly assess the feasibility and implications of increasingly megalomaniacal IT projects - another symptom of institutional madness.

Symptomatic

I therefore see the debate about any special protection for hackers as whistleblowers, however well intentioned, as only a symptom. The government needs to “own” the information, to at least have the right to ask questions and to independently evaluate the answers to these questions. Or should we simply give away control of our sea dykes and hope that a few public-spirited people will report the hole in a dyke on their Sunday off?

Failure after failure

Nothing can be leaked that could change the way the people in The Hague deal with these problems. Nobody loses their head, even after such a mega-failure as Diginotar: and in comparison the implementation of both the electronic medical records and the public transport Chip card pales into insignificance, but no doubt these projects also continue despite failure after failure.

The big one

What is necessary for a real breakthrough? Like I said years ago in a debate about the EMR: an event that is too terrible to ignore. Because that is always what it takes in the Netherlands to shift our political-administrative system down a different path. It is always susceptible to the pressures of existing commercial interests or the idea of a couple of people losing their jobs. The complexity of Dutch society and the economy might itself bring about that change: something like a national breakdown of hospital systems, or something like an exploding refinery in the Rotterdam area. There are so many vulnerabilities to choose from.

I suspect there is a 'sweet spot' in terms of deaths versus effective political impact. Somewhere between the Enschede fireworks disaster (23 dead) and the 1953 flood (1835 dead), so to speak. I share Rop Gonggrijp's analysis that after Diginotar nothing will change (because there were no deaths on TV).

We are waiting for the big blow that is strong enough to make real change possible. Only then will there be room for other people with more technical expertise, involving a much higher level of technical requirements and transparency of all the inter-related processes such as design, selection and implementation of new systems. Perhaps a cruel cyber-attack with cute little piglets (on YouTube: ‘Al Qaeda attacks internet with photo of adorable piglet’)?[62]

Originally a Webwereld column

7.6 Unsuitable

2011

Over nine years ago, I was talking to Kees Vendrik (a Dutch MP) about the broken Dutch software market. Not only was it impossible to buy a top brand laptop without buying a Microsoft Windows license, it was also impossible to visit many websites (municipalities, Dutch railways and many others) without using Internet Explorer.

OS to my liking?

The latter area has greatly improved and I can lead my life using my browser of choice on my OS of choice. However, I have to just swallow a Windows licence when buying a new laptop. Not much has improved in that area. Despite all the wishes of our Parliament and its related government's policies, our national dependence on products such as MS Office has not really diminished either.

Meanwhile, the technological seismic shift that frightened Bill Gates so much back in '95 (the web makes the operating system irrelevant[63]) is fast becoming reality. Almost all new developments discussed by IT power players and specialists are web-based or based on open specifications and the most commonly used applications are running quite well as service in a browser.

New dependencies

So while the 15-20 year old problem of software dependency is not yet solved (our government, with its tens of thousands of IT workers, is still unable to wean itself off the familiar Microsoft technology stack), its impact is becoming less relevant. Meanwhile, new dependencies based on cloud providers are promising to be even more detrimental.

Excessive use of proprietary software creates the risk of foreign manipulation and potential attacks on critical infrastructure (e.g. Stuxnet). But at least if your systems are attacked in this way, there are some ways to track this. If you are working on the computer that does not belong to you, that is based in a foreign country and is managed in ways you cannot know, it will be very difficult to have any control over what happens to your data.

Subject to US legislation

The old assumption that using local servers could be part of the solution, seems unfortunately to be an illusion. All cloud services offered by companies based in the US are subject to US legislation, even if the servers are physically in another country. And US law is now somewhat, shall we say, problematic. With no evidence, but with an allegation of involvement in ‘terrorism’, systems can be closed down or taken over - without any warning, or the possibility of adversarial judicial review.

The term ‘terrorism’ has been stretched so far in that anyone who allegedly breaks US law, even if they’re not a US citizen and even if they’re not in the US, can still a deemed ‘terrorist’ just on the word of one of the many three-letter services (FBI, CIA, NSA, DIA, DHS, TSA, etc.). The EU is not happy about this, but does not want to go so far as to recommending its citizens and other governments to no longer use such services.

The long arm of the US Patriot Act goes even further than merely the servers of US companies on European soil. Thus, domains can be ‘seized’ and labelled: “This site was involved in handling child pornography”.[64] Try explaining that as a business or non-profit organisation to your clients and (business) partners. Just using one .com, .org or .net extension as your domain name now makes you liable under US law.[65] All Europeans can now be seized from their homes for breaking US law. So a .com domain name makes your server effectively US territory.[*]

Unsuitable because of foreign control

We were already aware that proprietary platforms like Windows and Google Docs were not suitable systems for important things such as running public or critical infrastructure. However, now it turns out, that every service delivered through a .com / .org / .net domain places you under de facto foreign control.

Open source for things that matter

Solution? As much as possible, change to open source software on local servers. Fortunately there quite a few competent hosting companies and businesses in the Netherlands and Europe. Use local country domains like .nl/.de./.fr or, if you really want to be bullet proof, take a .ch domain. These are managed by a Swiss foundation[66] and these people take their independence seriously. WikiLeaks[67] ran a while on wikileaks.ch after its domains such as .org got a one-way ticket to Guantanamo Bay.

If you still want to use Google Docs, Facebook, Evernote, Mind Meister, Ning.com, Hotmail or Office 365 – please do so with the awareness that you no longer have any expectation of privacy or any other form of civil rights. Good for the administration of the tennis club, but completely unsuitable for anything that really matters.

Originally a Webwereld column, also on Huffington Post

* In the interview with Arjen by radio show 'Hell Radio', Arjen states (transcription):

"In your article you state, and I want you to explain what you mean by this to our listening audience, that if you are a European and you go to a website a .com, you are basically in American territory and you are subject to American laws. How is a .com website American sovereignty?

It happened de facto that when a British citizen had a website running on a .com address, when he hired a server that was physically located in the Netherlands, at some point an American company accused them of copyright infringement and then the US actually demanded from the British government his extradition to stand trial in America, under American law even though he was not an American citizen, his website was not running in America and the server was not located in America and he did not trade on America soil. Yet, the US government insisted that he should be extradited to the US to stand trial under the US law, when actually under European laws he had not broken any because the copyright laws are different here. It is that sort of stuff that is very troubling. The willingness to do a powerplay very hard combined with the big economic and military power of the US, makes it very hard for individuals and smaller countries to resist. So, one of the solutions is as in non-US citizen to basically avoid anything that touches the US, even though some of the services of some of the companies provide very value from a technical standpoint. For more strategic legal reasons it might be real consideration because of this behaviour as a non-American to completely avoid this stuff and take your things completely out of the US. This is of course a very bad thing for US business, so I am quite surprised that American companies have not pushed back harder on the US government to say: "Look, stop doing this stuff because you are going to ruin our business, because everyone outside the USA is going to walk away from us if this goes on and if this becomes more known and people start to think about this.'

We are discussing how .com are American sovereignty, how people who never stepped foot in the USA can be charged with breaking American law even though at no point they were in the USA. When I was reading that part of your writing, it made me think about the far right here in the USA and their fear of a one

world government being imposed by the United Nations. To what degree is the USA right now, especially when it comes to the internet, a one world government?

They certainly behave as if they do not have to adhere to any laws, regulations or agreements. I mean not even their own laws, let alone any agreement they may have with other governments. It is a sort of level of not caring about any agreement that they have with anyone, whether their own citizens, other governments, the UN Declaration of Human Rights, it seems anything can just be ignored as long as they state that they are doing it for national security. Of course, for most of us on the planet, that is not a very good argument. It does seem to be a logical extension of other activities that the US gets up to where they reserve the rights to essentially kill anyone anywhere. Since 2001 there is no longer a need for actual evidence or a trial or what we would all consider due process, for them to go out and kill people. That is pretty bad. When a single government that cannot be opposed by other governments because of their military might, simply asserts the right to do essentially anything to anyone anywhere - you know of course since Obama signed the National Defense Authorization Act (NDAA) now includes you as citizen, so it is now everybody - under the disguise of national security. It is quite worrying."

7.7 Asbestos is also useful

2011

For decades throughout the Western world, houses were built with asbestos. The material is affordable, durable, insulating and has also excellent fire resistant properties. All this - and the low price – made it the ideal stuff to use for everything. Which is what we did.

Do not touch

As long as the asbestos remains safely in place, nothing much happens. It does its job and you don't need to think about it. The problems begin when changes are made, such as a conversion. The demolition of such a wall releases microscopic asbestos fibres, resulting in enormous danger to the health of anyone who has the misfortune to be nearby. Consequently, the processing of asbestos is very strictly regulated. Despite these regulations, asbestos has caused twice as many deaths as road accidents for decades.

Social price

Because the long-term consequences of the use of asbestos is so damaging, its use is now prohibited. All this, despite the fact that the original reasons for using still exist: asbestos is still cheap, strong, durable, insulating and fire resistant. Yet we now do not use it because the social price is just too high. Strategic and social reasons are more important than practical and technical advantages.

"Everyone's used to it"

Yet when we talk about the software that governments use for their daily work, it seems virtually impossible to distinguish between strategic and operational arguments. Concerns about the fundamental inadequacy of closed (and uncontrollable) systems are easily dismissed by phrases such as "it's useful", and "everyone's used to it", or even "political concerns are not up for discussion". Asbestos suppliers also used all these quotes in the 1980s.

Desktop-monopoly

Fortunately, the traditionally cuddly but now dangerously naive Dutch approach to international relations was brutally interrupted last month: the Dutch government has been lying to itself and us about military deployment. People's cloud-computing data is indeed vulnerable; Israel and the USA use their technical knowledge of proprietary systems to attack their digital adversaries[68]; and 10% of Dutch PCs have been taken over by criminals. The latter is a direct consequence of the desktop-monopoly actively created by the government, and to this day strengthened through its IT-education policy.[69]

What is next?

Today it is an Iranian nuclear installation, the personal data of Rop Gonggrijp, and the domain of WikiLeaks. Tomorrow perhaps it will be a Dutch (air)port, power station, hospital or a few ministries?

A sound technology strategy

If the Netherlands wishes to retain control of its own sovereignty, we have to stop this quasi-naivety in conversations about technology strategy. Despite all international agreements, the law of the jungle still prevails, but we behave as if we are taking a stroll in the park. NOiV (or its successor programme) must find the courage to start a conversation about the strategic implications of running our public administration on systems that are not under our control.

It is time to strictly regulate our public sector asbestos-information. Although it can be useful, we must seek out alternatives that ware safe for everybody.

7.8 Cloud computing, from the frying pan into the fire

2010

In a recent column, Frank Benneker of Amsterdam University explored the consequences of the rapidly growing use of cloud computing. The shift of computer applications from PCs and servers to a single 'service' provided through a worldwide network is probably as fundamental a shift as the earlier one from mainframe computing to PCs.

Quick-and-easy

Given the objectives of the Dutch Open standards and interoperability policy plan, cloud computing seems the quick and easy-to-implement solution. I hear Web 2.0 enthusiasts say, "Put everything on Google Docs and we are all interoperable". However, just as in the case of the 'liberation' of PCs from mainframe managers/suppliers, there are problems with cloud computing – potential snakes in the grass.

Open standards for interoperability

In December 2004, the Dutch government decided that the dependency on dominant software providers was a problem and had to be addressed. The Dutch action plan from 2007 was the first, tentative step in dealing with this.

The Dutch government wants to use open standards for interoperability, and open source to foster independence, lower costs and strengthen local development (services instead of licences). Open standards are fundamentally essential for interoperability. The Dutch 'standard' government desktop plan demonstrates to governments that interoperability can also be achieved with an imposed, top-down monoculture. Give everyone the same software, and information can be conveniently exchanged.

The price of monoculture

However, the price of a monoculture is high, both directly in money and in less quantifiable aspects such as security problems and an extreme dependence on a few foreign private companies. The latter is especially difficult to reconcile with the idea of a sovereign nation and a government that is democratically accountable. Surely our governments would wish to avoid relying on foreign companies to control the connectivity of our information databases in some nebulous 'computer cloud'?

Crucial considerations

The crucial point is that even in this cloud, the hardware does not belong to the government nor is it possibly even on Dutch soil. The hardware can be located anywhere in the world, and therefore subject to multiple legal regimes beyond the Dutch government's control (or indeed, accountability).

Much of the Web 2.0 knowledge for the Dutch government and discussions about this were held on ning.com (ambtenaar20.ning.com) servers, and the consensus is that it would be pretty difficult to migrate away from there. Even NOiV, the Dutch open standards and open source implementation bureau holds regular discussions on LinkedIn instead of on its own environment.

Same, same

It is only natural that people use what they know. However, bearing in mind not only the objectives of the Policy Document, but also the various Parliamentary Motions on the subject and the earlier decisions of the government itself, cloud computing is a major IT problem. To expect cloud computing to rid us of the issue of 'lock-in' that has been a problem for the last 20 years, creates a classic example of 'out of the frying pan; into the fire'.

A separate IT

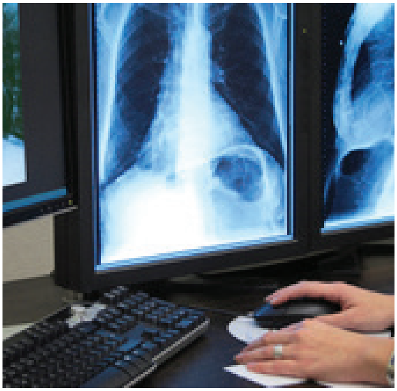
Our current problems arise from not foreseeing the long-term consequences of our IT choices. We need a separate government IT programme to ensure the freedom of choice that we see as entirely natural in other markets. Unless the cloud-computing servers are on Dutch soil and we have access to the code under an open source licence, we shall only go from bad to worse.

The Free Software Foundation[70] has the solution for these problems, a distributed cloud[71] that we can all access. Servers that provide free software designed to guarantee our digital freedom. After all, this is the original intention of the internet: all equal players in their own cloud.

7.9 When surgeons and IT architects work together

2010

The Dutch Journal for Surgeons, published an article written by my collegue Younass and myself. We wrote this article to further explain some of the points we made during our keynote at the national Convention of Surgeons. Younass Aboulghit and Arjen Kamphuis



We live at a time when information technology is drastically changing our lives. We can see the digital process all around us in information systems and the change in our working procedures. People always expect to be able to get information quickly and share it with each other if it is important.

Professionalism

In healthcare, there are opportunities and a new generation of patients has high expectations. The question is, how do we embrace the potential of information technology while maintaining quality and professionalism? How do we prevent the indiscriminate use of IT making the work of the specialist more difficult, rather than easier? That things can go badly wrong with healthcare projects has been demonstrated with the case of the Electronic Health Records (EHR).

IT to solve problems

EHR and related IT projects in healthcare often confuse medical and logistical functions. Different groups within a health institution experience different problems that they want to see solved through IT. Non-medical planning and logistics work is often an important way to improve the efficient use of workers and resources. However, from the perspective of front-line healthcare providers, this can mean that they feel treated like a cog in a machine, and this does not fit with their sense of professional autonomy. Certain lessons of the logistics of care can be drawn from the tailor-made principles of 20th century industry. However, a hospital is not a widget factory and a patient is certainly not a widget. The factory metaphor is useful, but also has its limitations. And, by not recognising these distinctions, software vendors and corporate buyers over the last 20 years have often gone wrong.

Central or decentral

The fundamental problem began with the introduction of the national EHR. Since the mandatory imposition of a national administrative system was considered unfeasible, the decision was taken to centralise and maintain the existing IT systems from 9,000 health care institutions as efficiently as possible. Merging all these systems into one structure was a political and administrative nightmare.

Reliable information

Unfortunately, the quality, speed and reliability of the overall national EHR relied on the standards used by each of the individual 9,000 institutions. A critical care professional cannot make decisions based on medical data of questionable reliability. Since no one knows how all these institutions store potentially relevant data about a specific patient, nor how reliable the information is, care professionals are reluctant to use the system. Gendo raised this fundamental problem back in 2005 after a test hack of two hospitals initiated by writer and privacy campaigner Karin Spaink. Now the First Chamber has quashed the idea of a national EHR, the field is clear for local and regional initiatives to apply lessons learned.

Large-scale not suitable

A mistake often made in healthcare is the implementation of large-scale IT systems basically not designed for healthcare. These systems compel hospitals and care institutions to align their processes to the IT rather than vice versa. This ultimately leads to a lot of frustration among service providers. We need to listen to the medical professionals who rely on IT systems in order to perform their job. A successful system should be based on a clear answer to the problems it solves. What are the needs of different stakeholders? Besides a clear definition of the problems, it is very important that stakeholders agree on the way forward. In other words, a shared IT strategy.

Best practice

A clearly defined strategy can be learned from the experiences of the St Anthony Hospital, which in 2008 began to build its own EHR based on open standards and open source software. The St Anthony consciously chose a longer route where the problem was not fixed by an external supplier, but developed its own solution. One of the steps the hospital took was to establish a steering committee consisting of different types of caregivers. Together they defined the vision and controlled the implementation. The principal reason for choosing open standards was the guarantee of future interconnectivity with other systems and organisations. The choice of open source makes it possible in future to develop new systems jointly with other institutions, without one party having all the control.

Cross-pollination of knowledge

The healthcare professionals most closely involved in developing the system need to be assured that they are actually helping their business. Both IT workers and health professionals need to be interested in each area and have the patience to learn. IT professionals are not surgeons, but can understand the problems of surgeons; good surgeons can grasp the basics of IT architecture, learning how to use it without the IT worker having to be present. Only through cross-pollination of knowledge is it possible to create solutions appropriate to both the medical and IT technical reality.

Reliability

Medical information is complex, and careful handling of patient information is a legal and moral obligation. The IT systems that process such information must be reliable. To ensure reliability, the IT architecture has to meet certain requirements, such as modular, secure, transparent and easy to audit, scalable, reliable and interoperable. To make these architectural requirements a reality, proven methods and components must be used. Transparency is achieved by using open source and providing proper documentation. IT systems need to be scalable and have built-in redundancy to allow for a comprehensive backup, recovery, and restoration strategy. To ensure that different IT systems can communicate with each other, they should be based on open standards like DICOM and HL7 messaging for information processing and image sharing. In addition to the above, it is also important that the architecture complies with the laws and regulations laid down for health care institutions, such as NEN7510.

Small, modular an interoperable

One of the goals of an IT strategy is a vision of the method of software development. An important part of the development philosophy is always to start small and modular. The basis for this is discrete units - blocks - performing one very simple function, that are interoperable with other blocks. By such a process of small steps, we can clearly prevent out-of-control monster projects costing many millions.

A system that has modularity as a design principle will always remain future-proof: new or individual modules can be added to adapt to new medical insights or changing legislation. Another important philosophy is to maximise the use of proven technologies and methodologies: in other words, use technological components where a consensus exists that they are reliable and future-resistant. The Unix OS is a common example of what can be achieved with this method of development. The UNIX family of operating systems currently runs TomTom, super computers, phones and all Apples (including the iPhone and iPad). For those willing to use it, the modular philosophy has proven to be flexible, scalable, secure and free.

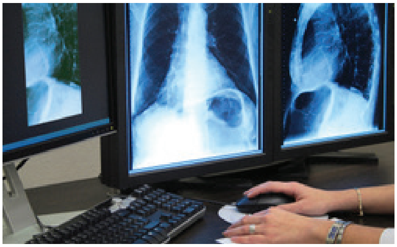
Collaboration

Building an EHR should involve close collaboration between medical professionals and IT architects, and result in compliance with key framework policies. The main challenge is for these two groups of professionals to explain clearly to each other their needs and expertise, and build an EHR structure, block by block, that will encompass everything.

7.10 Autoimmune disease in the pig pen

2010

Computer viruses and palliatives against them are a growing threat to high-tech care. There is a classic solution for the old problem of a vulnerable monoculture: diversity.



A virus

Recently alarm bells went off in many IT departments. A viral infection on Windows XP computers was initially caused by an anti-virus update from McAfee. The update made part of the system appear to be a threat and software for system file protection made the system unusable, a type of autoimmune disease.

Incompatible with new version

In hospitals and care institutions XP is still widely used, as specialised medical applications are often not ready for the new Windows version (and as often purely because of under-investment). This time it was McAfee, but almost all anti-virus products from time to time cause such problems. Anti-virus updates are a real-time arms race. And sometimes in the rush things goes wrong.

Efficient but vulnerable

From agriculture and ecology we know that monocultures are efficient but also very vulnerable. It is no different in the pigpen of IT. The management of 4,500 identical systems seems simpler than a more varied infrastructure – until a virus or autoimmune disease outbreak. Then the overtime starts. The scale of many of these incidents shows that even large health care institutions do not have proper internal firewalling and compartmentalisation. Nevertheless, the situation is better than five years ago.

Security-issues by monoculture

Security-issues caused by monocultures are not a new story. In 2003, Daniel Greer and Bruce Schneier wrote a report[72] about the security implications of the dominant OS monopoly. Since that time, neither the market nor the government has succeeded in effectively breaking this monopoly. In health care applications with medical or laboratory equipment included, many are Windows-only.

Conditional usability

Vendors often set additional conditions on the PCs, for example no firewall, before guaranteeing proper functionality for of their own applications. Thus a computer virus (or an autoimmune disease) is not only annoying for the admin department, but can also make scanners unusable. The MRI scanner can still take images, but the PC is crucial to the operation and viewing the results. So a Philips or Siemens unit worth a cool million is effectively scrap metal and patients cannot be treated. Sooner or later, this is a real time problem and then many more people than just the helpdesk are affected. In England, more than 1100 National Health Service computers were infected[73] with a data-thieving worm. And there goes your medical confidentiality.

Immaturity

From the many conversations I have had in recent years with IT workers, I conclude that the difference between a product monoculture (a 'standard' desktop) and the application of standards to achieve interoperability is still not understood. Some years ago, I spoke to a ministry official who enthusiastically told me that a 'standard' desktop was going to be implemented for the entire government. When I asked what standards would be applied, he launched into a list of products, "This version of an OS, this version of a word processor" and so on. The perception is prevalent amongst many IT managers that systems can only work and be properly managed if they are all from the same vendor and version. However, this is much more a symptom of market failures and the immaturity of the IT industry. It is a problem to be solved, not a law of nature to which we have to adapt.

It can be overcome

That there is another way to do things, can be seen from the work over the past 10 years in the Antonius Hospital in Nieuwegein. There they have consistently, in small steps, consciously worked to minimise dependence on a particular vendor, platform or application.

What most IT managers of health institutions describe as 'impossible' has been done in Nieuwegein. Fortunately, this hospital is in the centre of the Netherlands so when a really big crash occurs all critical patients can be sent there. We can avoid succumbing to the first virus or 'software-update-gone-wrong' by using virtualisation, web enabling and open standards environments to build greater diversity and interoperability.

Originally a Webwereld column

7.11 London is your Oyster

2008

The Oyster card is an electronic debit card that has all but replaced tickets on the London tube and bus transport systems. It allows users to put money on the card and discounts this credit as the card is used to enter and exit the underground and buses. The system is fast and unobtrusive and almost everyone who uses London public transport has one. Everyday millions of pounds are being put on these cards and taken off again as Londoners move about their city. The security mechanisms that are supposed to be keeping these millions (your money ultimately!) safe, have now been shown to be, frankly, utter crap.

Warnings, warnings, warnings

So the Oyster card has been definitely compromised. It is fundamentally broken and needs to be replaced by new technology concepts. Independent experts warned about this back in 2004 so there is no excuses for being all surprised now. Then they warned again in 2005 and in December 2008 at the Chaos Computer Club international IT conference in Berlin. Now the attack on the lacklustre security system of the London Oyster card has been practically demonstrated last April by a group of Dutch researchers who were investigating the same technology that was about to be implemented nationally in the Netherlands. "The Oyster card system uses the same chip and has the same basic vulnerabilities" according to Professor Bart Jacobs of the Computer Science faculty of Nijmegen University.

Cloning funds for free travel

After the publication of some of the inner workings of the data-encryption mechanism of the chip used in the Oyster card last December in Berlin, many experts predicted a fully operational breach. With the basic knowledge of the inner workings of the chip available online for anyone to see, implementing a working attack against the system was just a matter of time. The Dutch research group has been able to clone the funds on an Oyster card to another Oyster card. This provides at-home top-up mechanism allowing essentially free travel in the greater London area after an initial investment of 10 pounds plus a few blank Oyster cards at 3 pounds each.

Since the required devices and software are otherwise pretty much free today or in the near future (at most a few months from now), the London Transport Authority needs to get moving on this or accept that they will be providing free travel for those capable of using a laptop and a high-end mobile phone (and all their friends).

Classical hallmarks of public sector IT screw-ups

The systems failure bears all the classical hallmarks of public sector IT screw-ups. Basing your security mechanism on trying to keep the inner workings of such a system a secret while at the same time distributing 12 million copies of said system into the hands of the public is, frankly, insane. Does anyone think a handful of engineers locked in a room at

Philips can come up with a system clever enough so that the combined expertise of 1 billion internet users cannot defeat it? One has to wonder what they were smoking that day. Then there are bonus points for ignoring repeated warnings from independent experts for several years.

Security by obscurity

Among security professionals it is considered scripture that the only systems that can be trusted are those that have been tempered in the fire of public scrutiny. No one is as clever as everyone, and with a few million interested specialists online, there is nowhere to hide for a system containing design flaws. Flaws are always found sooner or later and most often sooner. One would think that after six decades of spectacular failures, the method of keeping a system secure by trying to hide its inner workings (know in the security trade as 'Security by obscurity') would be utterly invalidated. The Germans used this method for their supposedly secure communications using the Enigma machine in World War 2. It cost them the battle for the Atlantic and ultimately the war (ok, ok, attacking Russia in August without winter coats for the troops was not a smart move either). More recently a 16-year-old Norwegian hobbyist broke a $400 million DVD encryption method.

The Times picked up the story, and has a write-up of the wider security implications (access cards to buildings and such).

The Dutch system will probably not be implemented in its current form, but the London system is already operational with an estimated 12 million people using the card. For the sake of the financial stability of the tube system, one can only hope that clever engineers have already been working on a solution that can be implemented quickly. But I am not holding my breath.

7.12 Get a famous fingerprint

2008

The German Chaos Computer Club, the oldest and largest hacker group of Europe, made available to the public[74] the fingerprint of the German Minister Schäuble for the Interior. They wanted to show how easy it is to obtain someone's identity when identity is based on fingerprints.

National database with biometrics

The German government is preparing to build a national database containing the fingerprints of all its citizens for the purposes of fraud-prevention and national security.

Minister Schäuble is very angry about the release of his fingerprints and has stated he will take legal measures against the CCC. Dutch hacker Rop Gonggrijp pointed out that the Minister›s anger was curious since it was the minister after all who wanted to collect the fingerprints of over 82 million Germans and the CCC only collected one.

In your face

The CCC has been demonstrating for several years how easy it is to 'steal' someone's fingerprint and use is to fool all kinds of security measures such as payment systems, physical access controls and computer security systems. As with the doomed RFID cards, these demonstrations need to be very 'in your face' before media and governments take notice. Worldwide there are over 200 million devices in use of the 20 different types that were fooled by the CCC experts. As with the 100 million RFID cards they are all essentially worthless as serious methods for securing transactions or granting access.

Technically imcompetent

It is curious how we as citizens are constantly required to trust governments to handle our most private data when these governments often are not that trustworthy[75] themselves and also not very technically competent in guarding our information. Passports are easy to fake, RFID cards are easy to copy, and fingerprint readers can be fooled. Before we base our entire lives on these technologies, we had better make sure they actually provide a minimum level of security. For now, I am sticking to encrypted mail[76] and strong passwords.

Be Minister Schäuble

German TV broadcast an item about the possibility of stealing a fingerprint and using it to go shopping at someone else's expense at a large German supermarket chain. Since the TV piece did not include the entire method for making your own fingerprints I include it here. As with the RFID cards, these vulnerabilities have been known for several years, it is just that some companies and governments are a bit slow in picking up on them. If you want to go shopping as Minister Schäuble, just click on the picture at the top and follow the procedure from the movie.

Useless evidence

Update: A friend and IT security expert pointed out that since anyone can now pretend to be Minister Schäuble, which pretty much makes his fingerprint useless as evidence in court.

Maybe we should all publish our fingerprints (and retina scans and DNA profiles) to gain plausible deniability on future accusations of anything …

7.13 Public Transport card fully hacked

2008

What experts foresaw[77] last December and the Dutch research institute TNO denies was possible in their recent report ('Security Analysis of the Dutch OV-Chipkaart'), has been done. The deepest level of data-encryption on the NXP MI fare RFID chip has been hacked. Cash from cards can now be copied to other cards through cloning and that makes this system utterly unsuitable for serious applications involving real people and real money.

"All is well"

Essentially this is old news. The more interesting news as far as I am concerned is the fact that TNO was immediately rehired by the company implementing the card system to do more research on the validity of the hack. You have to wonder what the thinking is here. This company dropped the ball on at least three separate occasions in this area, so why do they get another chance to write a big rapport to claim 'there is no problem'? In addition, this is not the first time; on the sensitive subject of voting computers (now banned in The Netherlands), they also kept telling us "All is well".

Use a picture

If you merely want a paper to reassure yourself just ask the secretary to print out a pretty picture from the Interweb with a caption that says “Everything will be ok”. That is a lot cheaper then hiring a company like TNO, and apparently just as valid.

Does TNO just write down whatever the customer asks of them, or do they really not know any better? Either alternative is troublesome. As an important expert-adviser to the governments, we should hold TNO to a higher standard. When faced with an impossible request from a client they should respectfully decline the job explain that the client’s request is either technically impossible or not in line with laws concerning citizen privacy and such.

Rehiring

Our government (and parliament!) allowing such organisations to indirectly guide technology policy is a real problem that will continue to cost us dearly (in real money, privacy violations, theft and missed technology opportunities).

Next up for big IT-projects is a road-toll system that should allow for more flexible costs of (pay-as-you-go) owning and using a car. Hopefully it will not be as insecure as this project. That could be expensive for government or the citizen (or both).

The independent experts (the ones that got it right from day 1) have decided to boycott the upcoming meeting in parliament on this matter, since they are not allowed access to the ‘secret’ paragraph of the most recent TNO rapport. They wisely refuse to legitimise more ‘security-by-obscurity’ bullshit.

8.

About Open standards/ Open source

—

8.1 Letter to Parliamentary Committee on Gov. IT projects

2014

Letter below has been submitted to the Temporary Committee on Government IT. This document is a translation from the Dutch original.

Dear Members of the Committee on ICT,

On June 1 2012, I was invited by your predecessors to contribute to the expert meeting of the Parliamentary Working Group on ICT projects in government.

As an IT architect but also as a concerned citizen, I have been actively involved with the IT policy of the government since 2002, focusing on the areas of electronic health records, security and open standards/open source software. On the latter issue I was the initiator of the 2002 Parliamentary 'Motion Vendrik' that advocated greater independence from dominant software suppliers. Last year I also served as a technical expert on the Committee of Minister Plasterk (Committee Report Electronic Voting) who advised on the (im)possibilities of electronic support for the electoral process.

Although this motion Vendrik from 2002 was translated into the Heemskerk Action Plan in 2007 (see my article 'Open source policy talk at SigInt2010), this policy was quietly killed in 2010/11 by the lobbying power of large software vendors like Microsoft[78] and the U.S. government. Even the Court-of-Audit was pressured to *not* ask certain questions in its

2011 report (read my article ‘Docter, docter’) on the policy. Since 2002, the Netherlands has spent about 60-90 billion on foreign software, for which in many cases free, equally good or better alternatives are available. Their use is, however, actively hindered by both the Ministries of Education and Interior, as well as the VNG supported by the lobbying apparatus of major suppliers and the U.S. government.

This despite Justice Minister Donner’s 2004 letter to Parliament in response to the Motion Vendrik where he admitted that:

- the government’s dependence on Microsoft was very great;
- that this was a problem;
- and that it could be solved by introducing open standards and the use of open source.

This dependence has since become much greater and more than one billion Euro was spent on Microsoft licenses over the last decade. That money would have paid for 10,000 man-years of expertise to migrate away from Microsoft products. A large part of the money spent would have remained in the Dutch economy and returned to the state through tax and VAT. Not that 10,000 man-years would have been needed. The municipality of Ede did it against the odds for a fraction of the cost and now saves 92 % on software expenses (and 25% on overall budget). The rest of the government has yet to take steps. ‘Why’ is an important question.[79]

In addition to the huge amounts of money involved (the VAT ends up mostly in the Irish exchequer due to inter-EU trade to Irish headquarters of IT companies), it has also become clear in recent months thanks to Edward

Snowden[80] in particular that U.S. software is deployed as espionage infrastructure. This has practical implications. For example, the current semi-privatised infrastructure of the national Electronic Health Records system has been put under technical management of an American company and therefore falls under the Patriot Act. But the Windows PCs (which are de facto mandatory in secondary schools) and Gmail accounts (which are necessary to follow a university course) are part of the global spy network. Similarly with the iPhones that some of you might use, about which NSA internal documents boast of the 100% success rate in automated monitoring at zero dollars cost per device.

All this means that even if IT projects according to any definition 'succeed operationally', these often still violate the basic rights of millions of Dutch citizens (article 12 NL - Constitution, Art 8 ECHR, Art 12 UNDHR). Examples include electronic health records, transportation smart cards and many information processing systems of governments that have been outsourced on foreign soil and/or to foreign companies (such as the database of fingerprints that for many years has been linked to the issue of passports).

Both the EU and the Dutch government have been aware of this problem since the summer of 2001 (PRISM could have been avoided), yet nothing has since been done in the Netherlands to ensure the privacy of citizens or the data security of Dutch public and private institutions. Indeed, much has been done by the government that has greatly exacerbated this problem.

The above points, in my view, mean that a purely 'operational' approach to project success simply does not cover all the obligations of a democratic government in its role as guardian of the rights of its citizens.

This past weekend, I have viewed the first five videos of hearings and was most impressed by the contribution of Mr. Swier Jan Miedema. He seemed to be the only person genuinely committed to getting to the heart of the problems and saying out loud what he thought (although Prof. Verhoef also make quite a few wise points). The most compelling aspect of his testimony was the obvious fear of specifically naming a commercial party. This seems to confirm what many in the Dutch IT world know: companies like Centric abuse their dominant position in local government for short-term gain, including the exclusion of anyone who is a threat to those gains.

That an IT professional of such seniority has to beat around the bush with a trembling voice is typical of the situation in the 'market' for public ICT. Institutionalised corruption and abuse of power is more associated with a developing country than a democracy.

In the conversations with both Mr. Miedema and other experts, several members of the committee asked several times if these people could not suggest what would 'solve' all this. As if the problem was something that could be fixed with some trick. It is worryingly obvious that (two years and 8-12 billion after the start of the Commission) there is still the idea these problems can be solved by changing project-management methodology. Based on my experience, I believe that the problem is much more fundamental. I strongly urge you to look much more widely and more deeply at the problem and to not exclude your own role as parliamentarians in this. No questions or solutions should be taboo. Even if thereby the significant economic interests of above mentioned suppliers or the job security of groups of officials/civil servants must be called into question.

Both Mr. Miedema and Prof. Verhoef expressed the view that everything that happens can be broadly explained by the incompetence that exists in both the government and its suppliers. There are however, limits to the incompetence theory. Somewhere in the process the prolonged and appalling scale of wasting money, endangering the cyber security of the Netherlands and violating the privacy of millions of Dutch citizens has been allowed (or at least not considered an important subject). The fact that the Commission itself over the last 2+ years can spend a couple of hours a week on a problem that costs hundreds of millions of Euros monthly, might also be an indication of some inexplicable non-priority. There are many officials, businesses, cybercriminals and intelligence services abroad that greatly benefit from the status quo. Look especially at those who do not come to your hearings.

In the 21st century, laws are made reality by software. Therefore, it no longer befits a democracy to hand over control of that software to (often foreign) commercial parties. Executive parts of government must be accountable to you ultimately and without control over the technology that underpins their work this accountability is simply not possible.

Obviously I am willing to explain myself further as to above matters.

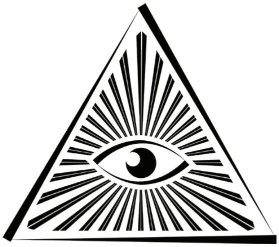
With kind regards,

Arjen Kamphuis

June 9, 2014: In The other IT of another Europe[81] I commemorate one year of the Snowden/NSA scandal by describing a scenario in which other choices were made, choices that are still open to us today...

8.2 The missed opportunity of avoiding PRISM

2013 – THIS ARTICLE IS BUILT ON 'UNSUITABLE'



On July 11th 2001, the European Parliament published a report[82] on the Echelon spy network and the implications for European citizens and businesses. Speculations about the existence of this network of Great Britain-and-her-former-colonies had been going on for years, but it took until 1999 for a journalist to publish a report that moved the subject out of the tinfoil-hat- zone.[83] The report of the EU Parliament contains very practical and sensible proposals, but because of events two months later across the Atlantic (9/11), they have never been implemented. Or even discussed further.

Sensible proposals

Under the heading 'Measures to encourage self-protection by citizens and enterprises' several concrete proposals for improving data security and confidentiality of communications for EU citizens are listed. The document calls on parliament to inform citizens about the existence of Echelon and the implications for their privacy. This information must be "accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology".

Encryption, open source and no back doors

Other gems are the requests to “take appropriate measures to promote, develop and manufacture European encryption technology and software and, above all, to support projects aimed at developing user encryption technology, which are open source” and “promote software projects whose source text is published, thereby guaranteeing that the software has no ‘back doors’ built in (the so-called ‘open source software’)”.

The document also mentions explicitly the unreliability of security and encryption technologies whose source code is not published. This is an issue that is a strict taboo in Dutch and UK discussions on IT strategy for governments (probably because certain major NATO partners might be offended).

Systematic encryption

Also, governments must set a good example to each other and their citizens by “systematic use of encryption of e-mails, so that in the longer term this will be normal practice.” This should in practice be realised by “ensuring the training and publication of their staff with new encryption technologies and techniques by means of the necessary practical training and courses.” Even candidate countries of the EU should be helped “if they cannot provide the necessary protection by a lack of technological independence”.

The basis for a solid IT policy

That one paragraph from the summer of 2001, when rational security policies had not yet been completely destroyed by 9/11, describes the basis for a solid IT policy that ensures security and privacy of citizens against threats from both foreign actors and the government itself (historically always the greatest threat to its citizens and the reason why we have constitutions).

PRISM could have been an American problem only

Had these policies been implemented over the last decade then the PRISM revelations of the last week would have been met mostly with indifference. European citizens, governments and companies would be performing most of their computing and communications on systems controlled by European organisations, running software co-developed in Europe and physically located on European soil. An American problem with an overreaching spy apparatus would have been just that, an American problem - like teenagers with machine guns or lack of universal healthcare, just one more of those crazy things they do in the colonies to have 'freedom'.

From the proprietary frying pan into the cloudy fire

Over eleven years ago, I was talking to Kees Vendrik (Dutch MP) about the broken European software market. Not only was it impossible to buy a brand laptop without having to buy a Microsoft Windows licence, it was also impossible to visit many websites (municipalities, railways and many others) without using Internet Explorer. The latter area has greatly improved and I can today lead my life using my OS and browsers of choice. The Dutch dependence on products such as MS Windows/Office has not really diminished however, despite all the wishes expressed by Parliament and attempts at government policies.

Today it is not possible to finish secondary school as a student without owning and using several pieces of proprietary software. Imagine making a certain brand of pen mandatory for schools and picking a brand of pen that comes with a spying microphone (not under control of the user). That is the current situation in practical terms in the Netherlands and UK amongst others. Germany, France and Spain are doing slightly better by at least acknowledging the problem.

Meanwhile, the technological seismic shift that frightened Bill Gates so much back in ‘95 (the web makes the operating system irrelevant[84]) is fast becoming reality. Almost all new developments discussed by IT power players and specialists are web-based or based on open specifications and the most commonly used applications are running quite well as service in a browser.

New dependencies

While the 15-20 year old problem of software dependency has never really been resolved (governments, with tens of thousands of IT workers, are still unable to wean itself off the familiar Microsoft technology stack), its impact is slowly becoming less relevant. Meanwhile, new dependencies based on 'cloud' providers are now proven to be even more detrimental.

Danger of no control

Excessive use of proprietary software creates the risk of foreign manipulation and potential attacks on critical infrastructure (see my article about Stuxnet, 'Cyberwar, the West started it'). But at least if your systems are attacked in this way, there are some ways to track this. If you are working on the computer that does not belong to you, that is based in a foreign country and is managed by people, you don't know in ways you cannot check, it will be very difficult to have any control over what happens to your data.

Post-9/11

The old assumption, that using local servers could be part of the solution, seems unfortunately to be an illusion under the post-9/11 empire. All cloud services offered by companies based in the US are subject to US legislation, even if the servers are physically in another country. And US law is now somewhat, shall we say, problematic. With no evidence, but with an allegation of involvement in 'terrorism', systems can be closed down or taken over - without any warning or the possibility of adversarial judicial review. The term 'terrorism' has been stretched so far in that anyone who allegedly breaks US law, even if they're not a US citizen and even if they're not in the US can still a deemed 'terrorist', just on the word of one of the many three-letter services (FBI, CIA, NSA, DIA, DHS, TSA, etc.). The EU was not happy about this, but until the PRISM leak did not want to go so far as recommending its citizens and other governments to no longer use such services. PRISM is making it possible to at least have a serious discussion about this for the first time.

US' long arm

The long arm of the US Patriot Act goes even further than merely the servers of US companies on European soil. Thus, domains can be 'seized' and labelled: "this site was involved in handling child pornography".[85] Try explaining that as a business or non-profit organisation to your clients and (business) partners. Just using one .com, .org or .net extension as your domain name now makes you makes you liable under US law (also see my article 'Unsuitable'). All Europeans can now be seized from their homes for breaking US law. So a .com-domain name makes your server effectively US territory.

We were already aware that proprietary platforms like Windows and Google Docs were not suitable systems for important things such as running public or critical infrastructure. However, now it turns out, that every service delivered through a .com / .org / .net domain places you under de facto foreign control.

Solution: open & local

Solution? As much as possible, change to free/open source software on local servers. Fortunately there are quite a few competent hosting companies and businesses in Europe. Use local country domains like .nl, .de, .fr or, if you really want to be bullet proof, take a .ch domain. These are managed by a Swiss foundation and these people take their independence seriously. If you still want to use Google (Docs), Facebook, Evernote, Mind Meister, Ning.com, Hotmail or Office 365 – please do so with the awareness that you have no privacy and fewer civil rights than English noblemen had in the year 1215.[86]

Fighting evildoers

A few months ago, a government speaker was defending the 'Clean-IT' project at a meeting of RIPE[87] (the organisation that distributes IP addresses for Europe and Asia). Clean-IT is a European project of Dutch origin, which aims to combat the 'use of the Internet for terrorist purposes'. The problem with this goal is that 'internet', 'use' and 'terrorism' remain undefined, nor does it seem anyone is very interested in sorting this out. This lack of clarity in itself can be useful if you are a government because you can then take a project in any direction you like.

Unable to secure

A bit like when data retention was rammed through the EU parliament in 2005 with the promise that it would be used only against terrorism - a promise that was broken within a few months. In Germany, data retention has now been declared unconstitutional and been abolished, while the Netherlands has rampant phone tapping, despite a total lack of evidence of the effectiveness of these measures. That all the databases of retained telecommunications data themselves become a target is not something that seems seriously to be taken into account in the threat analyses.[88] All rather worrying for a government that is still usually unable to secure its own systems properly or ensure that external contractors do so.

Outsourced & messed up

Also, during the lecture on Clean-IT much emphasis was placed on the public-private partnership to reassure the audience. It is strange that a government first makes itself incompetent by outsourcing all expertise, and then it comes back after ten years and claims it cannot control those same companies, nor indeed their sub-contractors. The last step is then to outsource the oversight function to companies as well and reassurance the citizens: “We let companies do it! Don’t you worry that we would do any of the difficult technical stuff for ourselves, it’s all been properly outsourced to the same parties that messed up the previous 25 projects.”

Access to all areas

‘Terrorism’ is obviously the access-all-areas-pass, despite the fact that many more Europeans die slipping in the shower or from ill-fitting moped helmets than from terrorism. Moreover, we as Europeans have experience of dealing with terrorism. ETA, IRA and RAF were rendered harmless in previous decades by police investigations, negotiations and encapsulation. This was done without jeopardizing the civic rights of half a billion European citizens. Even when IRA bombs were regularly exploding in London, nobody suggested dropping white phosphorous on Dublin or Belfast.

I hope that the pre-9/11 vision of the EU Parliament will be rediscovered at some point. It would be nice if some parts of the ‘Free West’ could develop a policy that would justify our moral superiority towards Russia, when we demand that they stop political censorship[89] under the guise of ‘security’.

Backup plan...

If all else fails (and this is not entirely unlikely) we need a backup plan for citizens. Because despite all petitions, motions, actions and other initiatives, our civil liberties are still rapidly diminishing. Somehow, a slow-motion corporate coup has occurred where the government wants to increase ‘efficiency’ by relying on lots of MBA-speak and corporate management wisdoms that worked so well for the banking sector. The fact that the government’s primary function thereby evaporates, does not seem to bother most civil servants. Meanwhile the companies themselves are apparently too busy making profits and fighting each other to worry about civil rights and other archaic concepts from the second half of the 20th century.

… DIY

So rather than always trying to influence a political system that so very clearly ignores our interests, we can simply take care of each other and ourselves directly. Do It Yourself. This conclusion may not be pleasant, but it gives clarity to what we have to do.

Encrypt

One good example would be to have educational and civil liberties organisations providing weekly workshops (crypto parties) to citizens on how to install and use encryption software to regain some privacy. These organisations should use their clout to get the slogan of “crypto is cool” on everyone’s lips. Technologists and designers should focus their energies on promoting the hip and user-friendly aspects of these pieces of software. This may be a lot more fun than lobbying ossified political institutions and actually provide some concrete privacy results.

Since 2006 I have ensured my own email privacy by no longer relying on the law, but by using a server outside the EU, SSL connection to it through a VPN tunnel entering the open internet also outside the EU. I encrypt as many emails as possible individually with strong crypto (using free GPG software). The fact that all those hordes of terrorists (who, our government asserts, are swamping the planet) have no doubt also adopted such measures - for less than 20 Euros a month – makes most of the low-level spying a complete and pointless waste of resources. Assuming the point truly is fighting 'terrorism' – something that is becoming a bit doubtful in light of the above.

Privacy, the last line of defence

Despite what some of the but-I-have-nothing-to-hide apologists say, we have privacy rights and other civil liberties for the same reason we have a constitution: not for situations where everything is OK, but for those rare situations where things are not OK. Privacy is the last line of defence against governments who lose sight of their reason for existing (to serve their people). Privacy is therefore not the enemy of security but the most basic part of it. Because governments are much scarier than any would-be cyber-criminal or even terrorists. Criminals may steal some money and terrorists may kill a few people but when it comes to wars, mass repression or genocide, you always need a government.

They know what to do

It is very obvious what European governments should be doing to promote the safety and security of their citizens and states. They already wrote it down in the summer of 2001. The fact that these measures are never part of any current ‘cybersecurity’ policy proposals, should make people very suspicious, at least of their governments’ competence.

The above article was originally written for and published on Consortium News. On June 22nd, I was interviewed by Chuck Mertz from ‘This is Hell!’ radio (Chicago, WNUR 89.3 FM). The entire program of that morning is on the This Is Hell! site. My interview (all 52 minutes of it) is here.[90]

Originally a column for Consortium News

8.3 Doublethink and Zen

2012

Doublethink[91] is a concept that was introduced by George Orwell in his famous novel '1984'. It is a mental mechanism that allows people to believe sincerely and simultaneously two completely opposing ideas without a problem.

No way to adoption

In the ten years that I have been involved with open source and open standards in the Dutch public sector, I have encountered many double thinkers. So for years I have endured 'experts' and insiders patiently explaining that the migration to open source desktops within that community would be impossible, because civil servants could not work with other platforms. Asking non-techies to use anything but the Windows + Office desktop they were taught at Dutch schools would lead to disaster. "It Just Could Not Happen."

Migrating

The certainty with which this (to this day) is mouthed as an aphorism everywhere, has always amazed me. Previously, the Netherlands had migrated from WP5.2 in DOS to Windows Word 6, yet the earth kept turning, children went to school and there was water from the tap.

Multiple migrations, mostly outside the Netherlands, have also demonstrated that ordinary users can do their work well with alternative platforms, provided they are given some training and support (something, indeed, that is perfectly normal when migrating to new releases of the usual proprietary systems).

Oh wait, there is way

The same people who for years have claimed with great certainty that "It Just Could Not Happen" have been busily rolling out iPads to the many managers and directors, who for many and varied reasons discover they need one. Apparently, the adoption of an entirely different platform with a totally different interface is not as problematic as was asserted for all those years. Huh?

Lax

The classic 'civil service desktop' tribe, led by IT heads of ministries and municipalities and supported by Microsoft, Pinkroccade and Centric, have had many happy years of 'standardising'[92] the Netherlands on proprietary tools, the management of which would then be done by the Dutch business partners of Microsoft. When asked why such a vulnerable and expensive monoculture was necessary, the standard reply is "working together!" For ‘working together’, according to these people, can only occur if everyone works with exactly the same stuff (never mind that millions of people on the internet are working together with very different tools). And that stuff should be consistent with what people already know, because learning something new is ultimately ‘not realistic’.

Contradictions

The Web 2.0-tribe wants everything on ‘the cloud’ so that with iPads they can ‘work together’ from Starbucks with colleagues and consumer-citizens-entrepreneurs. That this places control of state information in the hands of uncontrolled private and foreign parties, is not part of the discussion ‘We must work with the most modern tools!’ When asked what they do in concrete terms, the answer is almost always shifty or there is some muttering about experiments and the importance of ‘working together’.

Both of the above tribes mix at ‘e-government’-conferences and other such events and hear both perspectives, one after the other, with nobody apparently perceiving these contradictions. It is Doublethink in its ultimate form: simultaneously believing two contradictory ideas without experiencing a conflict: from 11:00 to 11:30 they can believe that a Microsoft monoculture is a necessary requirement for civil servants to ‘work together’, and then from 13:30 until 14:00 just as happily accept that all hip 2.0 workers, with their privately-bought iPads authorised via LinkedIn, must have access to the state-intranet, so that they are finally able to ‘work together’ with other officials. And nobody is pointing to the naked emperor and saying that at least ONE of these two stories has to be nonsense (and probably both).

Despite all this focus on collaboration between government organisations are regularly at odds, working against each other, re-inventing wheels 300 times, or point to each other when things go wrong. Even Caligula or G.W. Bush could still learn a thing or two from such levels of surrealism.

Vendors vs. expertise

Proprietary vs. open source in government is just ONE of the examples where sly sales representatives from dubious companies appear to be much more attractive than people with demonstrated expertise. Also in the cases of Electronic Health Records, voting computers, the public transport chip card and the security of its own systems, the government actively chose lying, cheating vendors and/or incompetent bureaucrats over its own citizens and academics with a proven expertise.

No diversity

After last year's 'Leaktober month' and the Diginotar drama, it appeared that some light might finally break in, but now it is clear that one deals with problems by treating them as an immutable fact of reality. With the logic of "as it is now, so shall it remain", the years-long impetus towards greater vendor independence and diversity of systems ground to a halt. Now the same logic is used as an excuse to defend failure everywhere. It is a bit like claiming to achieve fire safety by shouting that not every building is on fire, and anyway the fire engines can drive with 130km/hr away. “We react so quickly!” Prevention is seen as difficult and, moreover, “As it is now, so shall it remain, you will never be safe.”

Permanent state of doublethink

Despite this latest capitulation to foreign intelligence services and criminals, yet more megalomaniac IT projects are underway. Citizens continue to entrust the government with all their personal information, despite the fact that the government itself admits to being unable to protect them adequately. When working on such projects, you would need to remain in a permanent state of Doublethink to avoid a serious moral dilemma.

Doing nothing

Once the Netherlands had a government that built the Delta Works to keep the sea out and ensured that the country was ranked in the global top two or three in the fields of health, education, social security, security, democracy and transparency of governance. Only Sweden and Denmark sometimes did better.

Today feels like the Dutch government is abolishing itself. It knows nothing, wants nothing, does nothing. Perhaps we the citizens should do the same.

Give them nothing, ask for nothing, and expect nothing. The Zen of the citizen-government-relationship. Happiness is low expectations!

Originally a Dutch Webwereld column

8.4 It’s a trap!

2011

What is a document? It started as a flat piece of beaten clay, onto which characters were scratched with a stick. 8000 years later it was found and after years of study, archaeologists concluded that it said: *‘You owe me three goats.”*

From clay tot paper

Through papyrus and parchment scrolls, we arrived at mass production of paper and book printing in Europe in the 15th century. Our sense of the nature of a document is still derived from this previous revolution in information capture and distribution. When computers became commonplace as a tool to create documents, there was therefore a strong focus on applications to produce paper document as quickly and nicely as possible. The creation had become digital, but the final result was not fundamentally different from the first printed book in 1452, the Gutenberg Bible.

Digital paper

Most word processors in use today cling to this concept. There are hundreds of functions for page numbering, footnotes and layout to achieve a legible final result - on paper. Many IT tools around the management and access of documents, are directed to the concept of a digital document as a stack of paper. Ready to print for 'real' use. Paper is static, local, and now much slower and more expensive to transport than bits. The modern ways of working together for various reasons no longer apply to a paper-oriented way of recording and distribution. It is this combination of restrictions that has led to new ways of creating documents, where both the creative process and the end result is digital. A famous example is Wikipedia, the world's largest encyclopaedia with millions of participants continually writing and rewriting about the latest insights in technology, science, history, culture or even the biography of Dutch folk singer André Hazes.

In this new form, a document is a compilation of information at an agreed place online. The URL *is* the document.

Legacy

Most editors show their age not only by focusing on paper, but also by focusing on the concept that documents provide a discrete all-in-one storage medium. Word processing began before computers could communicate naturally through networks, and that legacy continues to shape the concept of a digital document.

#Intended

From the binary formats of Wordstar (.ws), via WordPerfect (.wpd) and Microsoft Office (.doc), we are now using XML-based formats such as ODF and OOXML. The original purpose of the ODF was to break the stranglehold of the Microsoft binary .doc-format, which was changed regularly and was therefore difficult to support on systems other than Microsoft itself. Of course, that was exactly the intention. Once you acquire market dominance, why would you be interested in whether other systems are compatible with you when this gives you the competitive edge and profit margins of 65%?

Digital asbestos

To my amazement, yesterday I read a report of a workshop designed to make OpenOffice compatible with the proprietary version of Microsoft's OOXML file format. The operational wish for individual OpenOffice users to be compatible with .docx is understandable, as they are a minority in a landscape totally dominated by Microsoft Office, which now saves documents as .docx. If you choose not to use MS Office (for whatever reason), it can be a daunting task to save and read a document.[93] Most users of word processors are unaware that, by using this format, they are making the lives of the minority difficult; they merrily continue to send out this digital asbestos.

For clarity, the .docx version of OOXML is not the same as the ISO version of OOXML. The format .docx is a proprietary file format, OOXML ISO is a standard. The certification of the ISO standard was itself nearly destroyed during the voting process by bribery[94] and intimidation. In 2011, the ISO standard has not been implemented by anyone yet, including Microsoft itself.

Disastrous path of the minority

Microsoft survives primarily on Windows and Office licences, even though it has doggedly been trying to conquer other markets such as mobile telephony. It would be rather naive to assume that such an organisation, with such a history, will sit back quietly while its cash cow is dismantled.

Solving problems of adoption of OpenOffice by pursuing the proprietary file formats of your opponent seems to me a disastrous path to go down. In the same way as the format .doc, the .docx-format can be subtly changed with each version and service pack 'upgrade' to avoid 100% compatibility. After all, actively tinkering with proprietary software to block alternatives is not a new concept for Redmond.[95]

Different is OK, if it is sexy

If the predictions about digital documents are true, it means we need new ways of working along with new tools. Page numbering and footnotes are irrelevant in hypertext in terms of the document-standard. Since the majority of documents produced by most users in most organisations are no longer than 1-3 pages and are usually using templates, a browser with plug-ins would be sufficient. This means that PCs are less important for the end users, who increasingly work just as well on a tablet. Tablets are very different to PCs, but that is no barrier to rapid adoption. Contrary to popular claims, ‘different’ is not a problem if it is also sexy.

Aping your opponent is never a good idea. As a great strategist once said long ago (in a galaxy far away): it is a trap!

Originally a Dutch Webwereld column

8.5 Docter, docter…

2011

A MP stumbles, coughing, into the doctor's surgery. There is blood pouring from the ears and nose and left eye.

"Doctor, doctor, I've just had a bad fall and I think I've broken my wrist" gasps the MP.

The doctor has a look and briefly feels the pulse. "Does that hurt?"

"A little bit" mumbles the MP.

"I don't think it's that bad," says the doctor, "Unfortunately I can't check it today as the digital X-ray machine is broken".

The MP is swaying back and forth. "It's probably just a bruise; the nurse will give you a sling. Take it easy for a couple of days and come back if it's still painful."

The MP staggers out of the surgery, still bleeding from the ears, nose and eye. The doctor is already focused on the file of the next patient, because doctors are very busy.

Wrong focus

The process described above resembles the way Court of Audit went about answering MPs questions about our national IT strategy. The MPs asking those questions were not experts and the Court provided simplistic answers without providing any context or stopping to consider whether the symptoms might be part of a broader problem. The newly published report failed to respond even to the superficial questions and, moreover, based its answers on minimal data. Which is a disgrace, as it is precisely the role of the Court to delve into the deeper issues.

Explore a different approach

Instead of focusing on the 88 million Euros spent on licence fees (less than 1% of the total annual licence expenditure), the Court could and should have explored why a different approach can work in other European countries, but fails in the Netherlands. Is this country really so different from Finland, Germany, France or Spain?

As their colleagues in the Central Planning Bureau had done in 2009, the Court could have produced its own qualitative analysis of the macro-economic effects of large-scale, open source implementations. This as a viable alternative to annual imports totalling of more than 8 billion, primarily from the USA. The macro-economic demand alone is relevant since the VAT and profit tax of this trade ends up predominantly in the Irish treasury, because of inter-EU trade regulations. (I am not necessarily against bailing out Ireland but this can surely be done more efficiently.) Also the figures of the 2004 SEO study are still current enough to be indicative for order of magnitude estimates.

Minimalist approach

As one of the 'experts' consulted by the Court, I am very disappointed by the minimalist approach it took. But perhaps I should not have been surprised – after all, in a previous report, the Court had also dithered, even after they had determined the government really had no insight whatsoever into its own IT spending. It is beyond me why a subject such as IT, where so many aspects can go so terribly wrong, is not more thoroughly and strategically overseen. In my written input to the Court last year, I proposed several clear ways to frame the fundamental questions. For those who are - like doctors - very busy, here is a summary:

Dear MPs, the Netherlands is a modern western country with access to the same knowledge, technology and IT budgets as Germany, France, Spain and Finland. Today all these countries have already achieved widespread adoption of open source and open standards in government. The work of the Dutch government is also very similar to these countries - certainly generic aspects such as office automation. So, eight years after the original and unanimous vote by parliament, surely the only reason that the Netherlands cannot implement this policy is our administrative culture and our Atlanticist political orientation Maxime Verhagen. There is certainly no fundamental reason why the results of the other countries I mentioned, cannot be replicated in the Netherlands, particularly because those same countries have already done the entire preliminary research for us. But in recent years, potential obstacles for migration have been elevated to norms rather than being correctly identified merely as part of a problem to be solved.

Parliament should no longer accept high dependence on a supplier being invoked as an excuse for not making progress towards becoming less dependent on that supplier (as the government did in response to parliamentary questions in in 2004, 2006 and 2008). The high dependency is the problem that must be solved, not an immutable law of nature where IT departments are the powerless victims.

Parliament should no longer accept the acknowledged lack of technical and organisational expertise of the 60,000 government IT professionals (and its suppliers) as a valid excuse for the lack of progress. It is implausible that the Dutch state cannot find the requisite skills to replicate the results of its European neighbours. Any IT staff and management found lacking in the necessary skills to carry out the very reasonable requests from parliament should be retrained or replaced. Incompetence is grounds for dismissal, not a valid excuse to refuse to do the work.

Excuses

Of course there will be problems in unravelling this gigantic Gordian knot, created by decades of accumulated proprietary software. But the most frequently cited excuses for not making a start with OSS and OS, are similar to those used by asbestos manufacturers:

"Yes, but it is handy", "We have been using it for so long", "We are comfortable with it", "We know nothing else".

All factually correct statements, of course, but certainly not valid excuses to prevent us from finding an alternative solution.

If the government had started making these changes way back in 2002, as parliament voted to do, the cutbacks we are now suffering in education and health care would have been more than covered.

On this issue, the Netherlands seems to have been reduced to providing the frightening role for the rest of Europe on “How not to do it...” Too bad.

Originally a Dutch Webwereld column

8.6 Parliament's questions to the Court of Audit

2010

Preamble

The Lower House of the Dutch Parliament has asked the Court of Audit to investigate the problems and opportunities related to the adoption of open standards and open source software for the government's information systems. The Court has invited various experts to give their views. This blog post is my contribution.

Ministry of Economic Affairs

The Netherlands in Open Connection

An action plan for the use of Open Standards and Open Source Software in the public and semi-public sector

Responsibility

The questions are being asked to the highest supervisory body of the country, rather than to the departments responsible for implementing this policy – the Ministries of Home Affairs, and also Economic Affairs, Agriculture & Innovation – eight years after the government's first unanimous vote on this issue and the expenditure of about 5 billion Euros on licensing fees. The impression given to the outside world is that Parliament is not impressed with the progress of the last eight years, and believes that the relevant government departments could benefit from the external scrutiny of a neutral and objective body.

Assumptions

Each of the following five questions implies a series of unspoken assumptions. In order to answer the questions, it is necessary to identify and, where necessary, challenge these underlying assumptions in order to reach a sensible answer.

The five questions

Here are the answers to the questions raised by Parliament. There is so much interdependence that subsequent responses will sometimes refer back to earlier parts.

"You cannot solve a problem with the same thinking that created it."

1. What possibilities and scenarios exist for the reduction of closed standards and the introduction of open source software by the central government (ministries and related agencies) and local authorities?

The Netherlands is a modern western country and has the same access to knowledge, skills, technology and comparable budgets for IT as Germany, France, Spain and Finland. It is a fact that all these countries have already implemented large-scale adoptions of open source and open standards in government. The implementation requirements of the Dutch government are also very similar to these countries. The reason that The Netherlands has not moved further in this area, eight years after the original, unanimous Parliamentary vote, can therefore be attributed to nothing more than the administrative culture and our Atlanticist political orientation.

No fundamental reason

There is no fundamental reason why the achievements of these other countries cannot be replicated in The Netherlands, especially as the groundwork has already been done. Barriers to migration have often been treated as immutable laws of nature rather than just a problem to be solved.

- **Address dependency -** Parliament should no longer accept that a high dependence on one supplier is an adequate excuse not to move away from that very dependency (as the Cabinet did in response to parliamentary questions in 2004 and 2006 and 2008). The dependency itself is the problem that must be addressed, not an enshrined principle that IT departments must endure.

- **Lack of knowledge is not an excuse -** Parliament should no longer accept that the acknowledged lack of technical or organisational knowledge amongst the 60,000 government IT professionals (and their suppliers) is an excuse for the lack of progress. It is implausible that the Dutch government is incapable of replicating the successful work of its European counterparts. Any governmental IT or management staff who do not have the requisite skills to carry out the very reasonable requests of Parliament should be replaced or retrained. Incompetence is grounds for dismissal, certainly not an excuse for refusal to do the necessary work.
- **Seek those with proper motivation -** Intrinsic motivation works better than coercion. Administrators and IT staff who understand the wishes of Parliament can embrace it with real conviction and are likely to want to produce better results than those who only work under duress. Such an approach will select and promote suitable people to the right jobs. The staff whose policies and behaviour have caused our current problems, are probably not going to the ones who find the necessary solutions.
- **Severe inadequate links -** The link between HR and remuneration policies for IT professionals and achieving technical certification related to proprietary software from a handful of suppliers, must be completely severed.

"When you find yourself in a hole, stop digging."

2. What part of closed standards and software can be replaced by open standards and open source solutions and what cannot?

This question has yet another unspoken assumption: that central government has a realistic oversight of all systems, applications and related standards. It does not. As a result, questions about the number of systems that can be replaced, are very hard to answer and have little relevance to achieving lower costs and greater independence in the foreseeable future – primarily because of the very large differences in costs that are associated with different standards. The government would do well to focus on the most common, generic issues, for which proven alternatives already exist. The original 2002 Vendrik Parliamentary motion already asked for this.

Key points to identify:

- What are the most expensive closed source areas where functional open source alternatives already exist and are already being used successfully elsewhere?
- What are the closest functioning areas that can result in successful migrations?

Migrate, just do it

Migration plans should be drawn up in these areas as a matter of high priority – and this means halting or delaying other projects that may block these migrations and accelerating projects that play a supporting role.

For instance in 2005, the former Ministry of Economic Affairs produced a document management system, which has made it virtually impossible for years for the ministry to use other web browsers, word processors or desktop operating systems. This is particularly surprising as, in 2004, the government itself announced that such closed systems in the work environment were harmful and undesirable, and were therefore going to be actively addressed as per the wishes of Parliament.

A current, concrete example within national government is the introduction of SharePoint. There is a significant risk that this investment, once made, will be (ab)used yet again as an excuse not to migrate to open and available alternatives. That would take us up to 2016 (14 years after the initial Parliamentary decision!) before any real work could begin on migration.

"Not everything that can be counted counts, and not everything that counts can be counted."

3. What are the current costs? What are the predicted up-front and structural costs, costs of moving from closed standards and the introduction of open source software? What are the projected savings?

The Dutch government currently spends about one billion Euros on proprietary software licences annually. These licences are mainly foreign, and the income tax and VAT on this expenditure flows into the Irish exchequer, because most European branches of American software companies are based there.

Unsustainable costs

The total Dutch expenditure is eight times more. Both governmental and general software expenses grow by about 10% per annum and are therefore unsustainable.

A significant portion of these annual costs can be saved or ploughed back into the local economy through Dutch SMEs, and so this cost will be an investment in the Dutch knowledge economy. With the government as the leading customer in this new market structure, it is feasible that the Netherlands could save billions per year.

In addition to these direct costs, various indirect savings could increase this amount many times over: the costs of management and security for vulnerable monocultures; the cost of merging old legacy systems and new applications; and social costs caused by security failures and easily avoidable software security problems. Regularly there are Dutch hospitals whose primary processes are severely disrupted by computer viruses – a direct result of monoculture.

Social implications

Moving beyond the financial, it becomes more difficult to quantify the social impact of the high dependency level of Dutch society on certain foreign, privately owned companies. However, if more than 80% of the

PCs in The Netherlands can be remotely controlled or even switched off, what does that say about Dutch national sovereignty? Is it politically acceptable for foreign software suppliers or government bodies to have an on/off-switch for ministries, municipalities, police, hospitals, water works, supermarkets, schools, etc.?

"The best moment to plant a tree is 25 years ago, the next best moment is now."

4. How would the reduction of closed standards and the introduction of open source software be realised?

With not only the right mandate (which Parliament actually voted for eight years ago!), but also the right expertise, significant results are attainable within 24-36 months. This requires making this area a priority issue and a break from the old attitudes, excuses and methodologies of recent years (see answer to question 1). Successes abroad can serve as templates for our projects.

Primary education, a good start

One area where we could make a rapid start would be primary education. Currently we are actively strengthening existing monopolies via this sector with public money. If by 2011/12 the first two years of primary school use open systems and then a higher class is switched each year, the Netherlands will have the first generation of citizens who are trained in vendor-neutral systems entering the workforce in 12 years, easily capable of working with multiple systems and applications. De 'Rosa Boekdrukker' primary school in Amsterdam clearly shows how this can be done.

Dutch hospitals in The Netherlands could follow the example of the Antonius Hospital in Nieuwegein. Many other hospitals can share in this success. And because it has already been shown to work, the risks and costs for the next 100 hospitals are much lower.

It will take at least a decade before the full potential of open source and open standards can be utilised.

"Go out on the limb, that's where the fruit is."

5. Beyond the cost, what other advantages, disadvantages, risks and opportunities should the Court of Audit factor in? What conditions must be met to make possible the implementation of open standards and open source software?

Benefits & opportunities

- Savings of billions per year in direct costs for all citizens and IT-using organisations in The Netherlands.
- Redirecting a stream of funds from Ireland/USA into Dutch society as a huge and permanent investment in our knowledge economy.
- Government investment in software will result in free, reusable software and knowledge available to our whole society, rather than controlled by privately owned and usually foreign companies.
- Security is strengthened through greater diversity of IT, competition, and the possibility of custom code audits.
- National sovereignty is reinforced when the government has complete control over its systems.

- General IT competence will dramatically improve, ensuring fewer spectacular and expensive failures such as the 2006 'Walvis' Tax project, national medical records, public transit chip cards and, most recently, the new police system to name but a few.

Disadvantages and risks

- The current, fragmented IT policy of the Dutch government means that a thousand little fiefdoms may need to be broken up.
- The apparent lack of skills amongst IT management may have consequences for personnel. No doubt there will be resistance.
- Significant investment is probably needed in re-training government IT professionals.
- Angry phone calls from Washington DC when the flow of licensing money is shut off.

Preconditions

- See answers to question 1.
- Be realistic about the positioning and motivation of software companies. Companies seek to maximise profits, control markets and will therefore exploit any leeway that the government offers them. We do not invite the turkey to discuss the Christmas dinner. Therefore why do we accept 'advice' from software companies and their interest groups about the best software strategy?
- We need to break away from the idea that extensive outsourcing is necessary, effective or desirable. The *raison d'être* of government is to justly serve the legitimate needs of its citizens; it should therefore

have detailed and inherent control over information systems. Stop the corporate-speak and 'playing business' by civil servants. Government is not a business, nor should it pretend to be. Outsourcing the control of information processing systems is contrary to the very principles of a democratic state for exactly the same reasons that outsourcing the military forces or the judiciary would be.

- Make a clear distinction between political and administrative goals and the means of achieving them. Cutting costs can be realised in many ways, regaining national sovereignty in only one.
- As long as desktop projects implemented under the guise of 'efficiency through economy-of-scale' result in each desktop costing 6600, - Euros *per annum*, this kind of bullshit-bingo is completely risible. Keep IT managers and other decision makers who do not know the difference between desktop-standards and a 'standard-desktop', away from such projects.

8.7 Open source policy talk at SigInt 2010

2010

I gave a talk at the 2010 CCC Sigint Conference in Cologne, Germany about open source policy. This is a summary of that talk. A direct link to the video of this talk on Vimeo: https://vimeo.com/13675382

Most European governments are busy migrating important components of their IT-systems to open source alternatives. The Netherlands was the first western country to develop a comprehensive policy for its entire public sector in 2007, but is lagging its neighbours in working implementations. The comprehensive policy in the Netherlands is focused on the practical advantages of open systems such as interoperability and lower cost and no vendor-lock, these reasons are also shared by policies in the UK and Denmark.

German, Spanish and French policies seem to have a more political dimension by also stressing national independence of critical systems and the possibility of code-audits as important reasons for going the open route.

By comparing Dutch progress (and sometimes lack thereof) with our neighbouring countries some lessons can be learned about what policies work and what some of the required conditions are for them to work in different political and IT-legacy environments.

8.8 Open source policy needs a 'Why'

2010

In 2002, Peru had a coherent action plan for open standards and open source. It went way beyond the Dutch action plan of five years later and was probably far ahead of its time. Where the strengths of the Dutch plan lie in focusing on practical operational goals such as interoperability, market forces and strengthening the local economy, the Peruvian plan did not attempt to hide its political mission.

Three clear goals

As Peruvian Senator Dr. Edgar Villanueva described in a famous response to a lobbying letter[96] from a proprietary supplier, these are the fundamental IT considerations for any democratic government:

- Free access to public data for citizens
- Digital preservation of data
- Safety of the state and its citizens

Accountability and preservation

The idea is that a democratic government must in the first place be accountable to its citizens concerning its actions. This makes control over, and insight into, the software that implements the law a political issue. Free access to public data and digital preservation are mainly the areas of open standards and it seems that this battle is pretty much won. The importance of open standards is generally accepted in 2010, even by the parties (you know who you are) that have actively blocked its implementation for many years.

Security of the democracy

Security of the state and its citizens is a lot harder. What security and against which threat? The state must protect itself from unwelcome outside influences. If it can be externally influenced outside the democratic will of its citizens, then there is not much point to democracy.

Full access to the source code is a good guarantee of a high level of control and independence. This access means the right to view, modify and redistribute those changes. The government must have, if it wants, its own 'gold master' to make critical pieces of software. With a certified, public checksum of the code so that a simple and transparent process exists for verification. This makes the government truly independent of foreign companies or countries that would like to exert influence through undocumented loopholes.

Protection of citizens

Citizens must be protected from both external and internal robber barons (this is why we have nation-states in the first place!), and against the government itself. Because we know that even democratic governments sometimes just lose their way when it comes to human rights, etc. This is why access to source code is also crucial. With an open platform you, the citizen, can protect yourself with heavy encryption on your data(traffic). In addition, someone can check that the crypto you trust does not have any back doors. Free software (also known as open source) is therefore just as natural as the use of open standards for any innovative, democratic and sovereign country that deserves the title. For a company this independence and freedom to innovate may also be a strategic matter. More and more companies are discovering that.

Business models vs. relevancy

Such a policy is not, as certain parties often state, discrimination against the business model or suppliers. The business model of a software supplier is not relevant to a government. But the terms & conditions of product delivery are and those may be set by governments. It is then up to the supplier to decide whether he wants to meet those conditions. Or not. No one is forced to deliver against their will.

Not the How, but the Why

The lack of a political mandate in the current Dutch policy is a limiting factor. Without a clear political strategy detailing the 'Why', IT discussions will always depend on migration plan details and total cost-of-ownership-for-3-years.

It may be totally against the zeitgeist to discuss the principles of democracy, national sovereignty and civil rights. But if we do not continually make these points, we might just as well outsource the governing of the Netherlands to Blackwater/Xe and Halliburton.

8.9 Open security, why it's the only way

2010

Keeping things secure is often associated with keeping things secret. "Don't tell anyone how the locking mechanism of the vault works, that will make it harder to break into it." The smart thief preparing a bank heist will of course take one of the engineers who designed the vault out for drinks and get him to spill the beans after a few bottles of something. The idea of keeping things secret to keep things secure is known as 'security by obscurity' and it never works. This is because it is very hard to keep secrets when many people knowing the secret (because they designed the vault for instance, or maintain or operate it) are just walking around being their normal human self. People like talking about their work or have a grudge against a former employer or colleague. Obtaining classified information if often a matter of just asking nicely (possibly while pretending to be somebody else). This is known as social engineering.

Because the fact that keeping-things-secret-to-keep-them-secure does not work is so counter-intuitive it is almost impossible to eradicate.

When steel vaults became communications devices and computers these old ideas persisted, even though they have been thoroughly disproven time and time again. In 1883 the Dutch cryptographer Auguste Kerckhoffs von Nieuwenhoff published are series of ideas about intrinsically secure information storage and communications by telegraph (the high-tech device of those days). His basic positions that the only secret in in secure system must be they key and all other components must be open for audit to as many experts as possible has been proven over and over again and remains true to this day.

History's lessons

The German Navy apparently did not read von Nieuwenhoff's work because the design of their cryptology device Enigma was based on the premise that its inner workings could be kept a secret from the Allies. This may be possible when there are only two or three devices and all are kept inside military installations but once you start putting hundreds of them on board submarines the chance of one of them being captured goes up steadily.

The capture of enigma by British intelligence and the clever misleading of the Germans by the Allies of the cracking of the Enigma codes is one of the great lesser-known stories of how World War-II was won. After misleading the German Intelligence into thinking the submarine U-110 was sunk with the Enigma on board (in reality it was retrieved by the crew of HMS Bulldog), British intelligence was able to keep the Germans convinced that their system was secret and thus secure. The German Navy and Werhmacht kept using the system for several more years while the Allies were reading their mail. This interception and decryption happened pretty much in real-time thanks to the early computers that were being built by the people at Bletchley Park (aka Station X). The ability to intercept and decrypt most German communications shortened the war by an estimated two years and was key to the success of D-Day. For the Germans of course trusting security-by-obscurity pretty much cost them the battle for the Atlantic and thus the war on the Western front (A great introduction to both the basics of cryptography and the history of WW-II information warfare is Neal Stephenson's page-turner Cryptonomicon). Since the secret has been out for a while, you can download your own paper enigma now.

This rather long winded lead in and history lesson is relevant today because having learnt nothing from all this companies and governments make the same mistakes as the Germans did 65 years ago again and again. And we get stuck with insecure systems that cannot protect our information, our money or us.

Some recent examples of the consequences of this kind of thinking are serious, others are funny.

So can we make systems secure, or at least secure enough? The answer is maybe. It depends on the applications, the acceptable cost and mostly the end-users of the system. More about them here.

Open security, it's the only way

It is now very broadly agreed upon by security experts worldwide that the only way to create reasonably secure systems is to have an open design and development process. This is the exact opposite of the vault manufacturer trying to keep the inner workings of the locking mechanism secret. In an open process, all available data on design and the actual implementation of it are shared as quickly as possible with as many experts as possible. This allows all those experts to study both design and implementation and point out possible mistakes and weaknesses to the persons building the system.

With many more brains working the problem, the end result is generally better than with a few isolated ones working alone.

Open the future

In software engineering this method has become known as ‘Open Source’. This refers to the public availability of the ‘source code’ of a computer program. The ‘recepy’ to make the actual software. Eric S. Raymond, one of the founders of the Open Source initiative formulated in his essay ‘The Cathedral and the Bazaar’: “given enough eyeballs, all bugs are shallow”. The idea being that any software engineering problem can be solved if enough different software developers work on the issue.

What Eric Raymond did was to reformulate a much older method for solving tough problems called the ‘scientific method’ or ‘peer review’. This is the formal method by which scientists keep tabs on each other’s work and challenge each other’s thinking. It is by no means a perfect system but overall the scientific method gets results. As a reader you are using dozens of them right now.

Information security, like many scientific problems, is very, very hard. Getting many people to work on the problem with you or for you is still the best way to ensure your system has a fighting chance. As Von Nieuwenhoff suggested 125 years ago: the only thing that needs to be secret about an information system is the key one uses to gain access, the rest should be open to peer review so as to be under permanent scrutiny.

The Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed set of testing methodologies that can be used as a framework for assessing strengths and weaknesses of information systems, protocols or things like physical buildings.

8.10 Hacking policy talk at HAR2009

2009

Had fun doing talk this afternoon at HAR2009. While I was taking a nap afterward, someone wrote a very nice review on the HAR-wiki.

I re-iterated many of the points I made at the CCC-conference in Berlin. My main points were also written down in English in a recent interview with the Indian Centre for Internet & Society.[97]

To spice things up a bit I added a new aspect about areas of public sector IT that should be under ultimate control by public sector organisations. I am still refining these ideas but this is the gist of it:

In modern nations, many laws and policies are implemented through software and supporting computer systems. Control over these systems is therefore control over the functioning of the state and its laws. A democratic government should therefore have total control over critical information processing functions, on behalf of its citizens.

Having access to the source code and the right to compile it into working binaries is a crucial part of this control. Examples of areas of application are voting tabulation, national defence & security, the police and justice system, power grids, *water and sewage systems, air-traffic, harbour and transport control systems and the national media.*

Open sourcing these critical government applications and supporting systems is therefore a required step for continued national sovereignty.

Thanks to Yolanda for taking the above picture and making it available.

8.11 Caribbean open source

2008

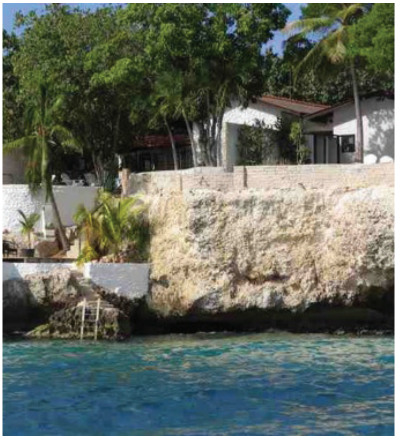
Last week I was visiting the Dutch Caribbean by invitation of the local government to do the opening keynote on their conference on open standards and open source. Curacao, one of the islands of the Dutch Antilles, is about to become fully independent nation state and that means a lot of re-design of the local IT systems of the government and public sector.

Determination

The government is determined to maximise the opportunities offered by open standards and open source software to move the new government, the local educational system and economy forward. An OLPC Project (One-Laptop-Per-Child) is being considered for education, because three PCs per school is not the way into the 21st century. Hopefully the new Internet Exchange (based on the Dutch one)[98] will bring down the cost of bandwidth so that all those OLPC's will be able to go online.

Expert knowledge vs. budget

It will not be easy to achieve all of this. Curacao is a very small entity to function as an independent nation and do everything themselves. There is a great need for expert knowledge and training to bring local IT-staff and administrators up to speed and the available budgets for this are very limited. Curacao spends about 20 million pounds per year on proprietary software licenses (mostly in government and other public sectors). This amounts to about half a month's wages per citizen. If this can be reduced by 30-50%, the budget required to make the desired changes is available (assuming the total IT-budgets can be kept at the same level for the time being).



Because this visit also included several meetings with local dignitaries and media appearances, I was invited to stay for a whole week in a beautiful apartment west of Willemstad. Many thanks to Ace Suares who has been working for open-IT on his island for many years.[99] He was the driving force behind the whole conference and a wonderful host.

8.12 Open source lobbying presentation in Berlin

2007

Just did a talk about my adventures in policy-land changing Dutch national policy on open source and open standards.

A five-year effort

On January 1st, 2002 I tried to use the website of the Dutch national railway (www.ns.nl) using Linux. The site refused me access, it was IE only. This sparked a conversation with members of parliament about the need for open standards. Over a five-year period I progressed from talking to opposition-MPs to meeting the economics minister directly and was able to significantly influence national policy despite total lack of funding or any specific mandate.

Success

On December 12th, we achieved a stunning victory, the Dutch public sector will move to standardize on Open Documents Format and use open source where comparable functionality is available in all new procurements as of 2008. Use of ODF as a public sector document standard will be mandatory in 2009.

From having no policy at all in 2002 the Dutch government has recently decided to mandate the use of open standards for all government institutions, health care, education, libraries and any other tax-funded organisations. Open source software will receive preferential treatment.

Why and how

My talk will tell the tale of why we did it, but mostly how we did it and how others can do it too in other countries around the world. How to get access to the power-that-be, how to get non-technical people interested in the subject. How to align your policy proposals with existing policies. I did a short lead-in with some of the political reasons for wanting open standards and open source in government IT, but the focus was on how to get results.

Coverage of the talk (German):
https://www.linux-magazin.de/news/linuxtag-2008-erfahrungen-aus-erfolgreicher-lobby-arbeit-fuer-oss/

9.

Random important stuff to help you understand Arjen’s message

9.1 What Europe needs to do after Snowden

2014 – THE KERCKHOFF LECTURE BY ARJEN

On Friday 13th of June 2014, I gave the Kerckhoff Lecture at the Radboud Universities Kirchhoff's Institute for information security[100] in Nijmegen. For an audience of students and faculty who probably know more about the math of cryptography than myself, I talked about the tech-policy implications of the Snowden revelations and why Europe has been doing so very, very little. I discussed the full scope of the NSA surveillance problem, the available technological policy solutions (see also 'The other IT from another Europe') and some suggestions about why ('Wat's it for? The objectives of policies & systems) they have not and are not being implemented (or even discussed).

Imagine

Imagine a whistleblower releasing detailed documentary proof of a group of companies that dump large volumes of toxic mixed chemical waste in European rivers and lakes. The documents describe in detail how often (daily) and how toxic (very). Now imagine journalists, civic organisations and elected representatives all starting furious discussions about how bad this is and what the possible horrible consequences theoretically could be for European citizens.

Now imagine that this debate goes on and on for months as slowly more documentation is published showing ever more detailed descriptions of the various compounds in the toxic chemicals and what rivers and lakes precisely they are being dumped into.

Now imagine that no journalist, civic organisation or elected representative comes up with a single concrete and actionable proposal to stop the actual and ongoing toxic dumping or to prevent future organisations getting into the habit of illegal dumping.

I am right there in the room, and no one even acknowledges me.”

~ Leo Cullum

Imagine also that both governments and public-sector organisations, including the ones responsible for health- and environmental matters continue to not only procure products and services from above organisations but also continue to give them the licences they need to operate.

Imagine that this goes on for month after month after month for a full year.

Now imagine it turns out that the government not only already knew about this 13 years before, but also had a detailed report on practical solutions to clean up the mess and prevent future poisoning.

Imagine that.

Inaction

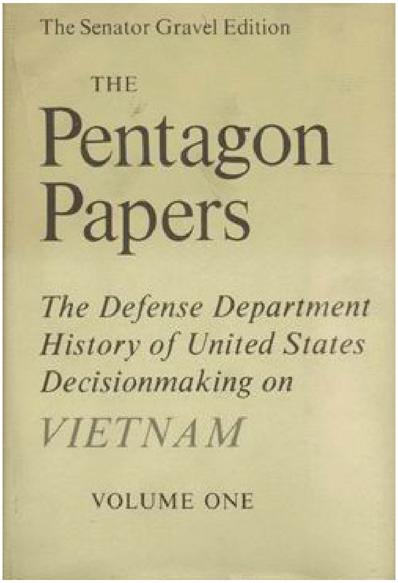
Sounds incredible, does it not? Except this is precisely how Europe has been not dealing with the revelations by Edward Snowden on industrialised mass-surveillance of our government & civic institutions, companies and citizens.

The EU has spent most of a year holding meetings and hearings to 'understand' the problem but has not produced a single word on what concrete actions could regain the right to privacy for its citizens now. This while a July 2001 report on Echelon[101], the NSA/GCHQ precursor program to the current alphabet soup, explained the scope of the problem of electronic dragnet surveillance and made practical and detailed recommendations that would have protected Europeans and their institutions had they been implemented. Currently only Germany has seen the beginnings of policies[102] that will offer some protection for its citizens.

Slides from this lecture are available.[103]

9.2 Xeroxing the war, dear journalists, get to work!

2012



The Senator Gravel Edition

THE

Pentagon Papers

The Defense Department History of United States Decisionmaking on

VIETNAM

VOLUME ONE

In 1969, when the Vietnam War was in full swing, a senior analyst at the US Department of Defence was quietly copying a secret report about the war. This report, which ran to 7,000 pages, covered the progress of the Vietnam War in exhaustive detail. The analyst intended to share this highly classified information with influential politicians and scientists, in the hope that it would quickly end the war.

That analyst was Daniel Ellsberg,[104] a former officer of the Marine Corps who worked for RAND, the Pentagon think tank. As a result of his experiences in Vietnam and his meetings with conscientious objectors in the US, he became convinced that the war was wrong. With his insider's knowledge, he already knew that it was militarily lost, but that the American government was misleading the people. Every day the Vietnam War took about eight hundred Vietnamese lives, more than two thirds of them civilians, and twenty American soldiers. Many more were seriously injured or maimed for life.

On June 13 1971, The New York Times tried to publish a number of excerpts from these documents, but was blocked by the Nixon government through legal and political means. Senator Mike Gravel[105] made a breakthrough by reading a large part of the document in the Senate. The reading of 4,100 pages took a while, but the rules of the Senate do not allow a senator who is talking, to be interrupted (the 'filibuster'[106]). Everything the Senator said automatically became part of the proceedings of the Senate and thus on the public record. The publication of this information was the beginning of the end of the Vietnam War and the start the process of withdrawal of US troops.

Fast forward to 2010. The US is once again embroiled in unwinnable wars, launched on dubious grounds, which continue indefinitely without any clear strategy or goal. Every extra day that these wars continue, more civilians and soldiers die.

And now there are new people who leak secret information about the wars, in the hope that the resulting political pressure will bring them to a close. The Xerox technology in 1969 has been replaced by a global computer network that uses encryption to protect the identity of the whistleblowers. Even WikiLeaks does not know their identities – this is safer for both the whistleblowers and WikiLeaks.

Off topic

However, the media's response is simply surreal. The bulk of the attention and the debate is about the Xerox machine – or at least the 21st century equivalent of it, the WikiLeaks website. Questions such as "Is WikiLeaks journalism?" and "Should you be allowed to leak classified information?" are discussed in exhaustive detail by apparently intelligent media pundits – who with alarming regularity seem to have little understanding of the very technology they are discussing.

Lying by the government

The first 'big' coup from WikiLeaks, the 'Collateral Murder'[107] video, led to a huge debate about the culpability of the helicopter pilots and whether or not it was reasonable for them to be able to distinguish between a camera and a grenade launcher. The key topic that was not discussed, was the simple fact that the Pentagon had knowingly, for three years, lied to both Reuters and the families of the civilian casualties in Baghdad about the circumstances surrounding the shooting by an Apache helicopter, which was one kilometre away and which riddled two children with bullets from its cannon. The Pentagon made a statement in 2007[108] saying that it knew nothing of any injuries to children, even though it had been in possession of this video from day one and it leaves nothing to the imagination.

The deliberate lying from the start of the Iraq war[109] continues to this day. The Dutch late night talk show, P&W, led the news on TV with "Dutchman involved in leaking attack video". That, after all, is news – apparently far more important than the fact that children were shot and there was a cover-up.

Wrong focus

WikiLeaks has already been the top story in the news for more than one week, and that is a problem. The Xerox machine is not important. Illegal wars of aggression launched based on lies are important. The torture of innocent citizens[110] in secret prisons[111] is important. Spying on UN diplomats is important. Messing about in the internal political decisions of other countries[112] is important.

So why is the entire media so busy with the Xerox machine and the person with his finger on the copy button?

Get to work!

Dear journalists, you have been presented with a cornucopia of scoops, many of which make Watergate pale into insignificance. If African dictators were doing the things Western countries are being accused of, they would be dragged in handcuffs to the International Court in The Hague.

Get to work!

Also on Huffington Post

9.3 Weapons of mass distraction

2010

On July 12, 2007 in Baghdad 12 civilians, including a Reuters photographer and his driver, were shot dead by a US Apache helicopter. Because of the involvement of the Reuters staff, this became minor news and the Pentagon gave a statement on the circumstances surrounding the events[113]: nine 'rebels' and two civilians were killed (the Reuters employees).

One way or another

That seemed to be end of the case. Reuters tried to research the circumstances of the shooting but was blocked by the US government. A formal request for access to videos of the Apache helicopter and audio communication between the crew and ground troops was refused. At that time the story was a tiny blip on the news radar, and quickly forgotten. There have been over 100 journalists killed in Iraq since March 2003 and an estimated 700,000 to over 1.3 million civilians[114] (the US military sees no need to keep track of exactly how many – "We do not do body counts").

Nearly three years later the incident is known worldwide because of the online release of 38 minutes of video recorded by the Apache helicopter involved in the incident. The shortened version on YouTube[115] has been viewed over 6 million times by now. For anyone who thinks the Iraq invasion was a good idea, watch the full 38 minutes.[116] Twice. A wealth of supporting information is available at collateralmurder.wikileaks.org. On Dutch TV, activist and hacker extraordinaire Rop Gonggrijp was invited to give some background to the video. The anchor closed the item with the immortal words "Well, it's a good story". Former Chief of Staff General Hans Couzy had called the actions of the Apache crew a war crime one day earlier.

Unexceptional bad behaviour

Immediately after the appearance of the video, heated debates erupted on a number of online forums. Was it reasonable or unreasonable to shoot? Or was just the first shooting reasonable and the second at the-bus-with-the-kids was not? The New York Times found it necessary for military experts to 'explain'[117], and to suggest with detailed analysis that really nothing was wrong. The 'rules of engagement' were followed and that you can't make an omelette without breaking eggs. Similar discussion took place in a multitude of other places. Many armchair generals who anonymously claimed military expertise stated that the behaviour of the Apache pilots were quite normal. How a badly injured person without any visible weapons can be a threat to an armoured Apache helicopter flying at least one kilometre away, remains unclear to me (take the time difference between the Apache firing its gun and the impacting of the shells and multiply this by 800 meters per seconds). Luckily, there are many veterans who honestly reveal[118] that the WikiLeaks video is unfortunately not exceptional.

The government knew... and lied

What was missing from virtually all discussion was the simple point that the original statement of the US Army from 2007 was incorrect and that they must have known that. On the day of the attack itself, the Pentagon had the video that we have access to only now. So how come they said for years they did not know how the two children were injured, as the crystal-clear video images show that the Apache helicopter shot them and their father for no reason?

Apart from the specific tragedy of 12 dead civilians and two seriously injured children, it seems to me the main lesson of the WikiLeaks video is that we are still consistently being lied to. The case for war in Iraq was based on deliberate lies[119] back in 2003 and it seems nothing has changed since then. To retain support in Europe for continuing the war in Afghanistan, the CIA has developed a great propaganda plan[120] in which the fears and principles of certain demographics in each country will be manipulated.

In The Netherlands, the Davids Committee report on the Dutch support for the invasion of Iraq expertly avoided the most important question: “Did we participate militarily?” by claiming that it *found* no evidence. It is unclear how hard they searched for that evidence, because more than enough has emerged in recent years. The easiest way to avoid annoying answers is still not to ask the question.

Soon on WikiLeaks, there will be a new video of a bombing in Granai,[121] Afghanistan. Hopefully, the discussion will not be about what type of bombs we can better use next time.

9.4 11-02-2014, the day we fight back

2014

Today is the 11th of February 2014,'The Day We Fight Back'.[122] We fight against out-of-control spying on our privacy as free citizens. We fight against Orwellian espionage because we know where it leads to in the end (first, they came for... and then they came for...).

The text below is inspired by the speeches of Winston Churchill[123] in during May and June 1940. While the nature of the opponents of democracy and freedom is different today, the consequences of losing the fight are just as dire. Our society and the planetary ecosystem is in great trouble. We need our democracies to function and our internet to be free so we can address the great challenges of our time.

What Cory Doctorow and Aaron Schwartz called the fight against SOPA & ACTA is over. The battle against TTP and global surveillance continues to rage on. Upon this battle depends the survival of the internet and our democracies. Upon it depends our own way of life and the long continuity of our institutions and our culture. Once again the whole fury and might of the enemies of freedom will very soon be turned on us now.

Those working towards a police state know that they will have to break us or lose this conflict. If we can stand up to them, all of the internet may be free and the life of the world may move forward into broad, sunlit uplands. But if we fail, then the whole world, including the United States and Europe, including all that we have known and cared for, will sink into the abyss of a new corporatist Dark

Age, made more sinister, and perhaps more protracted, by the lights of perverted technologies.

You ask, what is our policy? We can say: It is to hack, by server, laptop and phone, with all our might and with all the strength that Turing can give us; to wage lulz against a monstrous tyranny, rarely surpassed in the dark, lamentable catalogue of human crime. That is our policy. You ask, what is our aim? I can answer in one word: victory, victory at all cost, victory in spite of all the terror, corruption and lies.

I have, myself, full confidence that if all do their duty, if nothing is neglected, and if the best arrangements are made, as they are being made, we shall prove ourselves once more able to defend our networked homes. To ride out the storm of surveillance, and to outlive the menace of tyranny, if necessary for years, if necessary alone. At any rate, that is what we are going to try to do. That is the resolve of the hacktivists - every one of them. That is the will of free citizens, the technologists and the creatives, linked together in their cause and in their need, will defend their native internet, aiding each other like good comrades to the utmost of their strength. Victory, however long and hard the road may be; for without victory, there will be no free culture and no culture of freedom.

Therefore, we shall go on to the end:

we shall fight in Europe,
we shall fight on our browsers and our operating systems,
we shall fight with stronger encryption, and secure hardware,
we shall fight with growing confidence and growing strength,
we shall defend our networks, whatever the cost may be,

We shall never surrender.

Let us therefore brace ourselves to our duties, and so bear ourselves that, if the internet and its hacker community last for a thousand years, they will still say: "This was their finest hour".

Now go participate in or organise a cryptoparty, support people developing better tools (mail, web[124], secure systems[125] and all this free-as-in-freedom software[126]) or ask other people if they value being able to read without being read at the same time.

Privacy is a human right according to the UN Declaration of human rights[127] and yes, you too have something to hide as well[128].

9.5 NSA intel goldmine, who else has access?

2013

Shortly after the initial release of some documents from whistleblower Edward Snowden, I wrote a little summary about the IT-policy implications for Europe, based on earlier columns.[129] A lot of additional documents have come out since then and we can basically conclude that almost every computer system on the planet is fully broken or at least very vulnerable to NSA interference or manipulation.

Nobody, including the NSA, Edward Snowden, Glenn Greenwald has a total oversight of all the in the tens of thousands of documents let alone the political or strategic implications of the info contained in them.

Wrong focus (again)

Most of the news keeps focusing on the 'scandal' aspect and/or the person of Snowden. Being angry with the US government (practised by most opponents) and attacking the person of Snowden (a favourite of apologists of the US regime), distracts from defining adequate policy responses and so far there have been precisely none in Europe. This constitutes a massive failure of the various EU governments to protect their citizens' rights and the economic sovereignty of their nations. It is also strange in light of the fact that an adequate policy response had already been formulated in July 2001 and really just needs to be implemented.

But every now and then, the disinformation spread by some apologists for the behaviours of the NSA is useful for understanding how much worse the situation may just turn out to be. This article by a former NSA employee[130] is a nice example of an attempt at smearing the whistleblower while actually digging the hole the NSA (and the US regime) is in much, much deeper.

The piece claims Snowden secretly worked for Russian intelligence all along. While I do not share the authors views on Snowden's motivations or allegiances, the suggestion that outside organisations could have agents inside the NSA has some interesting implications.

Also on Huffington Post

9.6 On journalistic integrity

2013

This post text started as an email to a Dutch employee of the national broadcast service NOS[131] (somewhat equivalent to the British BBC) - Overview of this on Sander Venema's blog in English.[132]

Hi Jeroen,

Yesterday you felt it tweet-worthy that Russia Today TV (RT) had cut off a guest who used the platform he was given not to discuss the Bradley Manning trail but instead staged a protest against the horrible LGBT-rights situation in Russia. This incident was to you 'proof' that RT could not be trusted as a good information source in other things. As a reference, you picked the Dutch newspaper 'De Telegraaf'. This, in my view, was a rather unfortunate choice since this newspaper has itself a long and sordid history of collaborating with the German occupation, misinforming of misrepresenting world events and generally being a publication that only cares about human rights when it suits their political agenda. All in the tradition of FOX News and the Daily mail.

At OHM2013 I talked about implications of accelerating tech, some ways to understand the various crisis we are in right now and some questions we can ask about the strange things our governments seem to be up to these days ('future shock').

Wrong focus

I was critical of most western ‘mainstream’ media because they see quite incapable of asking basic questions such as: “Why are we putting Bradley Manning on trial and not the helicopter-gunner who shot up over a dozen civilians including children?” Shooting at children with an anti-tank gun and then lying about it to the world is probably a war crime, certainly something worth digging into in the context of a war that itself has been started based on lies.

Simply ask the right questions

After more than 10 years, the organisation you work for seems quite incapable to even come up with the proper questions relating to the greatest western war crimes since 1945 (let alone have the guts to ask them). This despite the fact that you are paid for, by the public, to inform that public about the world. This so we can make better-informed choices when we go to vote or protest the people we voted for last time.

It is the kind of simple question that RT.com *does* ask (or allows their guests to ask) on-air. And for this reason, I find them a good source of information/insight with respect to Western policies and activities. And when discussing getting good information on these policies I was asked what I considered a good source and so I said: “RT”.

I do not *prefer* using a Russian-state-funded TV channel to get my info about what the West gets up to in Asia or North Africa but the utter failure of organisations like the NOS (and BBC, etc., etc.) leaves me with a distinct lack of options. Instead of criticising RT for not being the news organisation you would like them to be, you really should look for solutions closer to home.

So for somebody like yourself, employed by an organisation that is supposed to ask tough questions but does not (for whatever reason) to use that single incident using that particular source to 'prove' a point is, to be quite frank, laughable and sad. Understanding that Twitter is not good for nuance my reaction to your tweet was therefore in kind.

Before and during OHM2013 I did several radio interviews, including with some of your colleagues. Every time I was asked if the hacker-community was a bunch of (cyber) criminals. This despite the fact that in 24 years of Dutch hacker events, not a single crime has been reported. I considered to reply with the return question if all journalists where corporatist warmongering whores. Obviously this would be somewhat hype as well but at least it would be hype with *some* basis in fact.[133]

During the interviews, your fellow journalists seemed to be most baffled by the fact that Julian Assange was happy to spend a full hour talking to our community, while they were getting no responses at all to their repeated interview requests. I hope the above shines some light on this situation.

You state your job is listening. I would suggest it is also asking questions and providing context. Taking half an answer out of a 45 min lecture seems to be neither to me.

Dare to ask

So about the listening (and asking questions); what is your view on the lack of questions being asked about proven NATO war crimes and the current war on whistleblowers & journalists? Would you ask the question:

“Why is Manning in prison, after being tortured (according to the UN), for informing us about war crimes while the perpetrators of said war crimes are free to fly/command more Apache helicopters?”

And if not, why not?

Given that my taxes pay your salary and our taxes pay for the bullets in those helicopters, I suggest pursuing these kinds of questions (on live TV if possible) might be a better use of your time than tweeting about the possible lack of journalistic integrity of a foreign TV channel. Then some of us might even start referring to you as a ‘journalist’ (a title that one needs to earn, just as ‘hacker’), instead of NOS-employee.

I look forward to hearing your views on these matters. Feel free to forward this mail (without edits of course, you would not want to look like a Russian censorist).

Also on Sargasso.nl

9.7 What's it for? The objectives of policies & systems

2013

When trying to understand current events with respect to the surveillance state, it is often more useful to look at the policies that are influencing the events than individual cases (although the individual cases often make up 'the news'). In many cases, there is a gaping chasm between the formally stated goals of a policy and their actual effects ('wars' on various nouns such as 'terror' or 'drugs' come to mind).

Evidence

Despite this, discussions about and opposition against are often argued from the rather fictional standpoint that the stated goals are the actual goals. Even if it is patently obvious that the policy in question does not further this goal, and that everybody smart enough to have some influence is aware of this. Opposition against misguided or destructive policies thus allows the parameters of the debate to be fenced-in by its proponents. It is pretty hard to win any debate if the other party can define (and re-define) the goal posts without a need for any evidence that these goal posts are reasonably placed.

When a pharmaceutical company wants to bring a new pill to market they need to show, in a series of transparently documented clinical trials, that the pill does what it is supposed to do and does not have (too many) negative side-effects. Evidence-based decision-making is the norm and while far from perfect this standard prevents useless or downright dangerous pharmaceuticals from entering the market and thus the bodies of humans.

What problem is being solved?

So when governments develop policies it is reasonable to ask: what problem does this solve? What new problems does it create? What proof do you have that your claims about these problems and their solutions are actually true?

Let's just assume for a moment that the people keeping these policies going have roughly the same IQ and information as you and I. They can understand the effects of policies even if these are completely different from officially stated objectives. It is believable (depending on your gullibility) that a policy that turns out to have the opposite effect that it meant to have will be kept going for a little while through administrative inertia. But at some point this stops being credible (there is a limit to what we can explain by sheer stupidity of policy makers – really, there is!). You can believe some of the policy makers are stupid some of the time, but it is not reasonable that all of them are completely insane all of the time for decades.

So when policies seem to have clear effects that structurally differ from the official stated goals, I would suggest that the policy is working just fine, its goal is just not what the stated goal is. To understand what the real goal of a system of policy is, we can simply look at its most obvious beneficial effects. What's it for? What's it good at?!

Let's look at the example of the clearly failed policy of 'The War on Drugs'. Since that paragon or trustworthiness Dick Nixon 'launched' it two generations ago, the global drugs market has exploded to a $500 billion enterprise, all of it outside any form of government oversight or control. Price and availability have dropped almost constantly over this time in the entire Western World, while potency has increased. The goal of 'banning' certain drugs from society has clearly and abjectly failed. In the process, most judicial systems of modern countries spend the vast majority of their capacity waging this war. This to the detriment of doing things like improving public safety or going after violent criminals, rapists or thieves.

So clearly this policy of prohibition is not working, for all the reasons alcohol prohibition did not work in the US in the early 20th century. So why keep it going? What are the upsides and who is benefiting?

Keeping the policy going

Obviously many people working in law-enforcement are benefiting (job security), privatised prison systems are benefiting (more business), governments looking for excuses to arbitrarily arrest people are benefiting. Banks where the billions are laundered are benefiting. So, lots of parties have an interest in keeping the policy going, even though it has patently failed at any of its original or (re)stated objectives. The only logical conclusion is that the real objectives of the policy are now to provide the various benefits to parties above.

Mass surveillance unsuitable for catching terrorists

Looking at the surveillance state from this non-naïve perspective; what are all the systems, organisations and procedures good at? PRISM and the wider tool set disclosed by Edward Snowden is obviously not very well suited to hunting down plotting terrorist masterminds. You, know, the really brilliant ones that can successfully defeat the entire multi-trillion dollar US air defence infrastructure armed with just a few box-cutters. People who are that smart, do not plan their operations on Facebook or use unencrypted Gmail accounts for communications (unlike certain libidinous generals tasked with hunting them). Many former intelligence and security services officials have stated that the way to fight terrorism is good old investigative police work and perhaps a serious look at the stated grievances that is the reason for the radical behaviour. This is how most European terrorist networks were successfully dismantled in the late 20th century. Finding a needle in a haystack is not served by adding hay.

Mass surveillance suitable for suppression

So logically, the goals of these programs are not ‘catching terrorists’ or preventing attacks, something they have never demonstrably done. But this does not mean that these systems have no use. They are of use and are being used for what they are good at: suppressing dissent in democratic societies. This is done by infiltrating and breaking up activists networks and thus pre-empting effective protest.

By labelling non-violent and legitimate political activity ‘extremism’ or ‘terrorism’ the entire suite of anti-terror laws erected over the last decade can be brought to bear against citizens using their democratic rights to protest various wrongs they perceive in society (human rights, environmental problems, governmental corruption, abuse of power by corporations, etc...).

True nature of surveillance

Therefore any realistic discussions on the nature of the surveillance policies we live under need to start from the understanding of the true nature of these systems and policies. It is not a mistake or polite difference of opinion on how to address ‘security’ questions. Effectively resisting these policies cannot be done from the quasi-polite and naïve standpoint of acceptance of the official goals.

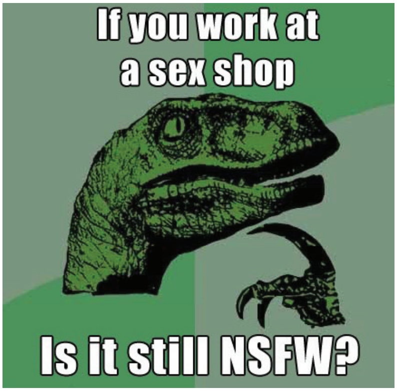
Those wanting to resist must show the policies for what they are; methods for achieving objectives that would never be accepted by the remaining democratic functions of western societies.

If all of this sounds too evil for your liking, consider that the alternative is the idea that the world really is run by spoiled toddlers. Not impossible, but very much more unlikely.

Column syndicated on Consortium News

9.8 Icelandic porn filter is overkill - about online freedoms

2013



In the middle of election season in Iceland, a debate is raging about the need to protect young children from violent pornographic imagery that can be found on the Internet. A proposal to put a national filter on Iceland's internet connection to block violent pornography caused quite an uproar in Iceland and abroad. Although it is unclear what the scale of this problem is, there is concern about the methods used by some in the porn industry to market their wares. There is an idea that some firms use the old tobacco industry method of get-them-while-they're-young'.

As I was in Iceland to give a talk at Reykjavik University on privacy and online freedoms, I was fortunate enough to be asked my opinions on these matters by government officials. The entire debate is being conducted during election season, so the local media are on top of every word uttered by anyone from either government or the local digital civil liberties organisations.

Internet filter

What causes most of the (international) attention is the specific plan to put a national filter on all Icelandic internet connections. This would be a first for a western democracy (although such filters have been tried in various Asian countries from Iran to China). Proposing a method that could very well be called censorship is incongruous in a modern and progressive society such as Iceland, which is the only country to have convicted its bankers over their part in the current global financial crisis.

Within a few hours of setting foot on Iceland, I was asked by Smari McCarthy of the Icelandic Modern Media Initiative to sign their letter of protest against the filtering proposal.

Emotions, problem, solutions

During an informal dinner a few days later with officials, it became clear that no decision on a filter, or any other policy, had been made. The government was looking into the problem and discussing possible solutions. The emotive nature of the debate causes the problems and solutions to be mixed up. I therefore attempted to structure the discussion over dinner.

Goals:

1. minimizing the harm caused by violent/degrading imagery to young children in Iceland;
2. fighting the industry that makes money out of degrading humans.

As stated, I think it is vital to see these as separate goals that may require completely separate policies. The first is clearly an Icelandic state issue, the second may require a multi-national approach, although there could be things Iceland can do to 'not be part of the problem by funding this stuff'.

Methods:

1. **A national filter.** The problem with a national filter on certain forms of internet traffic is that these filters work very poorly. This is because of the rapid speed of technological innovation on the supply side and the high creativity in circumventing the filter on the demand side. Once a filter-circumvention method has been found by one person, this knowledge will spread rapidly until it is everywhere. There are even special websites made by-and-for kids on how to circumvent filters and blocking software installed by parents/teachers/governments (their motto: "*It is not a crime to be smarter than your parents"*).

   So the Icelandic government would open up a two-front technological info-war against both the porn industry - the very people who invented things like video-streaming over the internet - and its own citizens, some of whom may have a legitimate (if hard to understand) desire to watch certain content. Aside from the fact that forbidding things that are not perceived by their consumers to be harmful, this also makes the forbidden fruit more interesting for young people developing their independence and testing the limits of society.

   But let us assume that someday in the future a filter is developed through a technical miracle (these sometimes do occur). Now you have built a working turnkey censorship infrastructure. The key question then is – who is actually in control of this infrastructure? Can you trust all possible future Icelandic governments or civil servants with the power to selectively turn off sources of information to all of Iceland?

In light of all the anti-terrorism laws being deployed against journalists, environmental and peace activists, and even citizens who fail to separate all their rubbish appropriately, this is not a theoretical problem.

2. **Away with the business model for the industry.** Now for the porn industry and options for taking it down (assuming for the sake of discussion that this could be a legitimate objective for a government). In my view the best and most practical thing that Iceland can do, is to be very minimalist and selective in enforcing US-style copyright. Cutting off the money supply is a very concrete and easy thing that much of the internet is already doing to the porn industry. Instead of frustrating this process, as many governments seem to be doing, the Icelandic government should welcome it. Thus making sure that those who want such online content can get it without sending money to these organisations. People make porn to make money. Take away their business model, and the business will go away as well.

I do, however, remain puzzled by one question: how precisely does the porn industry make money from kids? Do children have credit cards? I would find it hard to believe that these companies are doing things in the hope of a new customer 9 years from now. The tobacco analogy only goes so far: cigarettes are usually bought in cash, online porn with credit card or PayPal. The lack of statistics about the problem - How many kids have been affected: five? Five hundred? Five thousand? And how do we come by these numbers? - is also a problem.

Forbidden fruits vs managing the problem

Like drugs, porn and gambling will never be completely removed from society as long as certain people want them. But the problems they cause can be managed and minimised. Attempts at banning things are usually not the most effective way to reduce harm. Even the banning of 'child porn' (a complete misnomer as it is actually imagery of child abuse) has not clearly led to fewer children being harmed by the production of it. Production and distribution has gone so far underground, that nobody really knows what is going on anymore. The fact that researching/discussing these issues is a now a legal minefield does not help the situation.

Meanwhile these laws have provided a very nice way to destroy almost any individual simply by hacking their pc/laptop/phone (usually fairly trivial), putting some forbidden material on it and reporting them to the police. Even if they are not convicted and sent to prison, their career and social standing will probably be destroyed beyond repair. Proving one's innocence in such a case is nearly impossible.

Production phase is when the harm is done

The strangest point is that despite the heavy crackdown on images of child abuse, western police forces rarely take down known servers on their own soil. The idea that making imagery of child abuse (aka 'child porn') invisible by technical means somehow results in the reduction of harm to children is widespread. Despite the actual harm being done during the production phase of the material rather than during the distribution phase.

Hiding stuff or protect children?

Because the subject invokes such strong emotions, many politicians (and their staff) will often make a strange logical leap. It goes like this:

1. this problem is terrible, we must do *something*;
2. *this* (a filter, ban, deploying the army) is *something*;
3. we must do *this*.

In the process of formulating sound bites for the evening news, the fact that *something* may be completely ineffective in solving the problem and also has major negative effects on society is forgotten. We see these kind of mental illogical-leaps all the time in areas like 'the War on Terror', 'the War on Drugs' and 'Cyber security', where the solutions clearly fail and, in fact, cause massive new problems that are often worse than the original issue.

Much of the above casts serious doubt on the true goals and priorities of the government. Are we busy hiding stuff we would rather not see, or are we working on protecting children?

I have strongly suggested that the Icelandic government considers the above and uses any budget, allocated for filters, for improving sex-education in schools and support for addictions in the healthcare system. This may not yield immediate results but will most certainly do more good than implementing technical solutions that either do not work or make Iceland into an informational dictatorship. Update 2016: Despite a change of power, the debate over this continues in Iceland.[134] Strangely still with a complete lack of statistical info on the scale of the problem.

Originally a Webwereld column

9.9 Cyberwar: the west started it

2013

A few years ago, Israeli and American intelligence developed a computer virus with a specific military objective: damaging Iranian nuclear facilities. Stuxnet[135] was spread via USB sticks and settled silently on Windows PCs. From there it looked into networks for specific industrial centrifuges using Siemens SCADA control devices spinning at high speed to separate Uranium-235 (the bomb stuff) from Uranium-238 (the non-bomb stuff).

Isotopes needed

Iran, like many other countries, has a nuclear program for power generation and the production of isotopes for medical applications. Most countries buy the latter from specialists like the Netherlands that produces medical isotopes in a special reactor at ECN. The western boycott of Iran makes it impossible to purchase isotopes on the open market. Making them yourself is far from ideal, but the only option that remains as import blocked.

Vague insinuations

Why the boycott? Officially, according to the US because Iran does not want to give sufficient openness about its weapons programs. In particular, military applications of nuclear program is an official source of concern. This concern is a fairly recent and for some reason has only been reactivated after the US attack on Iraq (a lot of the original nuclear equipment in Iran was supplied by American and German companies with funding from the World Bank before the 1979 revolution).

The most curious of all allegations of Western governments about Iran is that they are never more than vague insinuations. When all 16 US intelligence agencies in 2007 produced a joint study, there was a clear conclusion: Iran is *not developing* a nuclear weapon[136] (recent speech by the leader of this study in on YouTube[137]).

And that is strange.

For if the 16 American intelligence services and their Israeli colleagues, the famous Mossad, can all agree that Iran is not making nuclear weapons, how do you justify an attack against civilian industrial infrastructure? And that this is the equivalent of a military attack is clear when you consider what would happen if Iran had been caught in a cyber-attack on 'our' installations in Borssele or Indian Point.

Attack on civil nuclear industry

Stuxnet is designed for a single purpose: the damage of nuclear enrichment facilities in Iran. This is a country that just may perform these activities in accordance with the international agreements stipulated in the Non Proliferation Treaty. Iran, like most other countries in the world (except Israel, India, Pakistan, S Sudan and N Korea) signed this convention. Nuclear weapons are not allowed but civil nuclear industry is. A detail that sometimes escapes the attention of editors.[138] Like the reason why Iran is not a democracy.[139] I am not saying the Iranian government are darlings, but the country has not attacked anyone in the past 200 years, unlike several of our NATO partners.

It does not matter

But Stuxnet has made some things very clear to Iran and the rest of the non-Western world. It does not matter that you abide by established agreements and treaties. It does not matter that you are not a threat to the West. It does not matter that the countries that accuse you most of violating the non-proliferation agreements (US and Israel) are themselves the most egregious violators; USA by delivering plutonium to Israel and Israel by not even signing the treaty and secretly stashing 100-200 nuclear bombs in the basement.

So there is no reason for you to stick to agreements or treaties, because it does not guarantee that the parties on the other side will do the same and it may offer a strategic disadvantage. In addition, if you going to have the disadvantage of alleged conduct (boycotts, threats of bombing), it is logical that you also want the benefits. It is almost rational for Iran to develop a military nuclear program. Certainly North Korea seems to get away with it. As a bonus, is now has a few nuclear weapons and that is still the best guarantee that the US will not be bringing unsolicited packages of 'democracy' (although a lack of oil wells also seems to help).

Escalation or de-escalation

Like the attack on Iraq, which was carried out based on deliberate lies (the US and UK knew Saddam had no WMDs[140]), the US again does not comply with the standards that it happily tries to impose on others. With the result that no one takes such standards seriously anymore and the world and cyberspace become a Wild West shooting gallery.

And that is exactly what you do not want in a world where a handful of angry Chinese / Russian / Iranian / Iraqi / <insert other country> can completely anonymously and in secret take down your critical infrastructure. Western countries are much more vulnerable due to their high degree of automation than countries that have just outgrown their third world status. Cyber weapons are relatively inexpensive and developing them is more difficult to detect than the construction of missiles and aircraft carriers. The best defence against it is the prevention of an arms race. Like a nuclear war, everybody loses in a cyber-war. Safety in such a context is created by moral leadership (starting with: follow your own rules) and actively working at de-escalation. That is exactly what the US and Israel have not done.

With such friends, we are assured of a continuous stream of new enemies in countries that mainly want to be left alone, but that arm themselves just in case the ‘free West’ is on the prowl in their region.

Setting up a Dutch Cyber Army while the sluices and pumping stations are equipped with factory-default passwords in their SCADA controllers, seems pretty stupid. If you live in a glasshouse, not throwing stones and not motivating others to do so, is the smarter move.

Update: a NATO research team has determined the Stuxnet ‹attack› against Iran was an ‘Act of Force’[141] (not an ‘Act of War’). We will see if that determination holds up if a non-NATO country (let’s say Iran) does the same to a NATO country.

Originally a Webwereld column,
also on Huffington Post, Consortium News and Globalresearch

9.10 Dining with spies

2013

At their yearly conference, the Dutch the National Cyber Security Centre stated this week they want to listen more to the hacker community. It is fine that the government will, at last, listen to the people who have been ahead of the curve for decades, although the question why it has waited to do this until 2013 remains. Even if this had been done as recently as 5 or 10 years ago, it would have saved an incredible amount of trouble and public money.

Consulting hackers

I sincerely hope that the consultations with the hack(tivist) community are about more than just technical tricks, because most benefits to society are derived from discussing policy (read ‘Privacy a decade on’). For purely technical issues the usual consulting companies can always be hired and then simply pay hackers for their knowledge and advice, just like any other experts.

Meanwhile a big group of hackers were unhappy about the fact they were not welcome and organised an alternative meeting. If the NCSC’s intentions for the coming year work out in practice, next time this might not be necessary. On the community side, these invitations to the table should be discussed openly and in detail (who sits at the table and wearing what hat). Because when community contributions and possible commercial interests are mixed up, things quickly degenerate into bickering and arguing. I speak from experience ;-). Nobody is 'representative' of the entire hacker community. The NCSC will have to adjust to the idea that we have no centralised organisation with a head office where you can meet up with the CEO/director/top-dog.

Political refugee

Unfortunately, I could attend neither meeting, as I had a dinner engagement in London. This took place at the Embassy of Ecuador, where Julian Assange resides as a political refugee from US government extradition. The dinner was held in preparation for the presentation of the 'Sam Adams Award for Integrity in Intelligence'[142] (award given annually to an intelligence professional who has taken a stand for integrity and ethics), to be held the next day at the prestigious Oxford Union Society. This prize is awarded annually to someone who has played an important role in the field of intelligence, peace and human rights. Some former prizewinners and organisers gathered in London ahead of the ceremony to visit Julian Assange (a former winner, 2010), as he cannot leave the embassy property without risking a one-way trip to Cuba, Guantanamo Bay. The US government has convened a secret grand jury to indict him for espionage (or just assassinate without process[143] - a perennial favourite). This despite the fact he has violated no US law - journalism is still just about allowed. The small Embassy of Ecuador in London is now probably one of the best-guarded places on earth, both visible (police-trailer-with-antennae) as well as invisible surveillance.

Speaking truth to power saves lives

The winner this year was Dr. Thomas Fingar, who in 2007 was responsible for coordinating the National Intelligence Estimate on Iran. Despite enormous political pressure on him to produce a desirable response, Dr. Fingar did his job and analysed the facts. The study emphatically concluded that since 2003 Iran had abandoned a nuclear weapons program. In his memoirs, Governor G.W. Bush (the title of president 'elected') admitted this report made it impossible for him to "use the US military to deploy against Iran" - you can hear the disappointed tone. Dr. Fingar's integrity saved lives, in this case potentially millions of Iranians and others in the region.

Eavesdropping

The sober (in terms of both atmosphere and alcohol) portion of the dinner was spent on planning the ceremony. After both the planning and several bottles had been dealt with, the conversation turned to the situation in the embassy. Naturally such a group will then speculate about eavesdropping by the former colleagues of tablemates Ray McGovern (CIA), Thomas Drake (NSA), Coleen Rowley (FBI), Annie Machon (MI5) and Ann Wright (US Army). Bugging devices in the walls and the ceiling through very slowly and silently drilled holes? Laser beams on the windows? Directional microphones from across the street? Microwave radar?

Write what you are not told to, journalists

Talking with a group of former spies and Julian Assange about all the different ways to be eavesdropped on is a sure-fire way to lose any and all illusions about privacy. Fortunately for now, such aggressive surveillance need only be of concern to people whom visibly and effectively speak truth to power. The power of intimidation - the pushback - used against you also provides a good measure of your effectiveness as an activist (or journalist). 'If you're not getting arrested every now and then, you need to try harder.' In the Netherlands we have too many reporters who write what others tell them to, and too few journalists who write what others tell them not to. Respect to the small group in the latter category.

Ceremony program blocked

The planned program for the award ceremony would be brutally swept off the table the following day by the Board of Trustees of the Oxford Union. The promised live streaming of video (and posting on the YouTube channel of the Union) was blocked at the last minute on vague grounds. Apparently a discussion between former intelligence insiders is threatening enough to suspend a centuries-long tradition of openness and academic freedom of speech. Clearer evidence of the need for WikiLeaks can hardly be imagined.

Update 1: A video clip of the speech of Julian Assange during the awards ceremony last Wednesday by the Oxford Union has been put online.[144] The background of the video (originally the helicopter video leaked in April 2010, read 'Weapons of mass distraction') is replaced by the logo of the Union (in some of the images filmed of the audience in the debating chamber, you can still see the original display). The official reason is that they are worried about possible copyright claims from the Pentagon (on a video that shows how journalists, citizens and children were shot with anti-tank weapons made from depleted uranium).

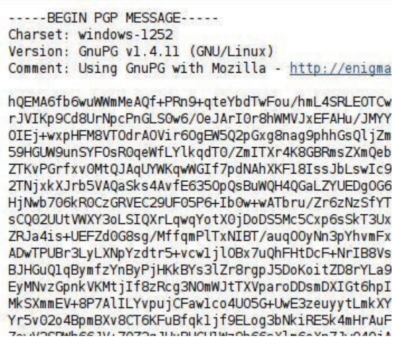
Update 2: WikiLeaks has published its own version of the speech.[145]

Footage of the speeches of half a dozen other attendees (including the recipient of the prize who was the point of the entire gathering) will hopefully follow as soon as possible. The Real News Network[146] has produced an overview of the event and its broader context. This will remain relevant to understanding current global politics for a long time.

Originally a Webwereld column , also on Huffington Post

9.11 Privacy, a decade on

2012



```
-----BEGIN PGP MESSAGE-----
Charset: windows-1252
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigma

hQEMA6fb6wuWWmMeAQf+PRn9+qteYbdTwFou/hmL4SRLEOTCw
rJVIKp9Cd8UrNpcPnGLS0w6/OeJArI0r8hWMVJxEFAHu/JMYY
OIEj+wxpHFM8VTOdrAOVir60gEW5Q2pGxg8nag9phhGsQljZm
59HGUW9unSYFOsR0qeWfLYlkqdT0/ZmITXr4K8GBRmsZXmQeb
ZTKvPGrfxv0MtQJAqUYWKqwWGIf7pdNAhXKF18IssJbLswIc9
2TNjxkXJrb5VAQaSks4AvfE635OpQsBuWQH4QGaLZYUEDgOG6
HjNwb706kR0CzGRVEC29UF05P6+Ib0w+wATbru/Zr6zNzSfYT
sCQ02UUtVWXY3oLSIQXrLqwqYotX0jDoDS5Mc5Cxp6sSkT3Ux
ZRJa4is+UEFZd0G8sg/MffqmPlTxNIBT/auqOOyNn3pYhvmFx
ADwTPUBr3LyLXNpYzdtr5+vcwljlOBx7uQhFHtDcF+NrIB8Vs
BJHGuQlqBymfzYnByPjHKkBYs3lZr8rgpJ5DoKoitZD8rYLa9
EyMNvzGpnkVKMtjIf8zRcg3NOmWJtTXVparoDDsmDXIGt6hpI
MkSXmmEV+8P7AlILYvpujCFawlco4UO5G+UwE3zeuyytLmkXY
Yr5v02o4BpmBXv8CT6KFuBfqkljf9ELog3bNkiRE5k4mHrAuF
```

On July 11th 2001, the European Parliament published a report on the Echelon spy network[147] and the implications for European citizens and businesses. Speculations about the existence of this network of Great Britain-and-her-former-colonies had been going on for years, but it took until 1999 for a journalist to publish a report[148] that moved the subject out of the tinfoil-hat-zone. The report of the EU Parliament contains very practical and sensible proposals, but because of events two months after publication (on September 11th), they have never been implemented. Or even discussed further.

Measures for data security and safe communications

The report lists under the heading 'Measures to encourage self-protection by citizens and enterprises' several concrete proposals for improving data security and confidentiality of communications for EU citizens. The document calls on Parliament to inform citizens about the existence of Echelon and the implications for their privacy. This information must be "accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology”. So not just some abstract government infomercial on TV/ radio, but hands-on tips to get some actual work done please!

Appropriate measures: encryption and open source

Other gems are the requests to “take appropriate measures to promote, develop and manufacture European encryption technology and software and, above all, to support projects aimed at developing user encryption technology, which are open-source” and “promote software projects whose source text is published, thereby guaranteeing that the software has no ‘back doors’ built in (the so-called ‘open source software’)”. The document also mentions explicitly the unreliability of security and encryption technologies whose source code is not published. This is an issue that is a strict taboo in Dutch and UK discussions on IT strategy for governments (probably because some major NATO partners might be offended).

Encrypted communication

In addition, governments must set a good example to each other and their citizens by “systematic use of encryption of e-mails, so that in the longer term this will be normal practice”. This should in practice be realised by “ensuring the training and publication of their staff with new encryption technologies and techniques by means of the necessary practical training and courses”. Even candidate countries of the EU should be helped “if they cannot provide the necessary protection by a lack of technological independence”.

Unfortunately to this day I cannot send encrypted mails to officials and the vast majority of them do not even digitally sign their emails to allow me to verify the integrity of the content. Despite the fact the software that makes this possible has been available as open source since before publication of the report in 2001.

That one paragraph from the summer of 2001, when rational security policies had not yet been destroyed by September 11th, describes the basis for a solid IT policy that ensures security and privacy of citizens against threats from both foreign actors and the government itself.

What a difference a decade makes…

Solid IT policy unknown

Recently, Privacy First organised a lecture & discussion evening on cyber security and the relationship with terrorism. Will van Gemert, director of National Cyber Security for the Coordinator for Counterterrorism and Security gave a lecture on the relationship between privacy and security. In this lecture there was much talk about consumers, little about people/citizens (perhaps the difference is a bit foggy from the windows of government skyscrapers in The Hague). He also insisted that the government is very much working with ‘the market’ and private parties. It was probably meant to be reassuring but had the opposite effect on most attendees. Ideas from the EU document from 2001 mentioned above, such as better IT education, open source encryption and technological diversity as defensive tactics, were unfortunately completely unknown concepts. The ribbon on the doors of the Cyber Security section of the National Counter Terrorism organisation had just been cut, so perhaps things will be better in a year. We can but hope*.

A few weeks earlier, another of our government speakers defending even more colourfully the Clean IT project at a meeting of RIPE (the organisation that distributes IP addresses for Europe and Asia). Clean-IT is a European project of Dutch origin, which aims to combat the use of the internet for terrorist purposes.

Terrorism is not defined

The problem with this goal is that 'internet', 'use' and 'terrorism' remain undefined, and there is not anyone very interested in sorting this out. This in itself can be useful if you are a government, because you can then take a project in any direction you like. A bit like when data retention was rammed through the EU parliament in 2005 with the promise that it would be used only against 'terrorism' - a promise that within a few months was broken. In Germany, data retention has now been declared unconstitutional and been abolished, while in the Netherlands we have rampant tapping, despite a total lack of evidence of the effectiveness of these measures. That all the databases of retained telecommunications data themselves become a target[149] is not something that seems to be seriously taken into account in the threat analyses. All rather worrying for a government that is still usually unable to secure its own systems properly or ensure that hired private parties do so.

Deassure

Also, during the lecture on Clean-IT much emphasis was placed on the public-private partnership to reassure the audience, yet this had a predominantly opposite effect. It is strange that a government first proves itself incompetent by outsourcing all expertise, and then it comes back after ten years and claims it cannot control those same companies, nor indeed their sub-contractors. The last step is then to outsource to companies that used as reassurance to citizens commented: “We let by companies do it! That you as a citizen do not think that we ourselves with our sausage fingers sit! Come all good”. After Diginotar, my confidence in the guiding and supervisory capacity of the government has dropped to just above absolute zero.

What a difference in approach between the summer of 2001 and today.

Access all areas-pass: ‘terrorism’

Terrorism is obviously the ‘access all areas pass’ - but many more Europeans die slipping in the shower or from ill-fitting moped helmets than from ‘terrorism’. Moreover, we as Europeans have experience of dealing with terrorism. ETA, IRA and RAF were rendered harmless in previous decades by police investigations, negotiations and encapsulation. This was done without jeopardizing the civic rights of half a billion European citizens. Even when weekly IRA bombs exploded in London, nobody suggested dropping white phosphorous on Dublin or Belfast.

Hope on the pre-9/11 vision

I hope* that the pre-9/11 vision of the EU Parliament will finally penetrate the Dutch Ministry of Security and Justice. (Formerly just 'Justice' soon 'Love'?) Perhaps a new cabinet will lead to new initiatives and opportunities? It would be nice if the 'free West' could develop a policy that would justify our moral superiority towards Russia, when we demand that they stop political censorship[150] under the guise of 'security'.

* *Hope: the desire for a future situation over which you have little or no influence: "I hope my plane does not crash."*

Originally a Webwereld column

9.12 Cybercrime; prevention vs. repression

2012

Cybercrime and cyber-warfare are currently the trendy terms the government throws around to acquire additional laws and powers. If it can also link cybercrime to the distribution of images of child abuse (also known as child pornography), the government has hit political pay dirt and can do pretty much what it wants. What continues to puzzle me is the answer to the question how all this focus on the distribution of such images actually protects the child victims themselves.

Police state

Bart Schremer published his opinion piece recently, providing an overview of the issues that law enforcement agencies are facing. On the one hand, society (or at least the media) expects law enforcement to solve all crime immediately, preferably on a modest budget. On the other hand, most Dutch people would still prefer to avoid a police state along the lines of the North Korean or American model.

Digital illiteracy

But in all discussions on permissible methods of detection, hacking police officers and crime-fight-using politicians is missing, is why cybercrime has grown so enormously. The fact that our reliance on IT is increasingly complex, will certainly have contributed. But one other important factor is the huge digital illiteracy among the vast majority of citizens. Aside from some half-hearted campaigns, the government has done little to teach citizens anything of real use or value.

If you have been online for a while (say more than 15 years in 2012), it is difficult to imagine that many internet users today do not know how a URL is constructed or what it does - and with today's browsers you do not need to know. I often see people typing the name of a site into Google (which is set as the homepage) and then clicking on it. And so, without batting an eye, they click their bank details through to helpdesk.br.ru/ING, or something similar. Just because the logo was in the mail, is it still the helpdesk of the ING bank? If people could understand the difference between a top-level domain and the rest of the URL, they could probably work out for themselves if the ING bank is really based in Russia.

Cybercrime because of ignorance

One of the main causes of the proliferation of cybercrime is the profound ignorance of most computer users. This ignorance is partly caused by an education system that teaches handy computer tricks rather than real understanding. The 'computer licence' is simply a course in MS Windows

& MS Office and provides no insight whatsoever into what a computer actually does or how networks function. Not that everyone needs to be a system programmer, but ensuring a bare minimum of understanding (such as the 'reading' a URL) could avoid so much pain.

In addition, the vast monoculture of computer systems is a major problem that the government is actively propagating. Thus, in the Netherlands, it is virtually impossible to finish high school without access to a system with MS Windows and MS Office. Running a school and getting it funded is even harder. Studying at many universities without a Google account is rapidly becoming impossible, and a Facebook account is required to function in other institutions.

The Lower House listening to the arguments, noted in 2002 that "software plays a crucial role in the knowledge society, and that the supply side of the software market at that time is highly monopolised". IT asked the government to fix this. This is the outline of the first sentences of the 2002 Vendrik Parliamentary Motion on the dysfunctional desktop software market. But this malfunctioning market aspect was soon forgotten in many discussions about various open standards and what open source web-system really is the best. But it did focus so primarily to a disturbance of the software market, not the internal management of secondary schools, municipalities and other public sector agencies.

A lot of hot air is wasted discussing nebulous cloud systems, but interaction with these clouds still occurs primarily via desktop/laptop systems. And the market for these systems remains almost as monopolised as in 2002. Whoever has control over these desktops, has de facto control over most information processing in the Netherlands. To date mostly criminals seem to be interested in our desktops. And because the desktop landscape of the Netherlands is an extreme software monoculture and this makes us vulnerable[151], and yet for the last ten years the government has done virtually nothing to reduce this vulnerability.

Vulnerable unpatched systems

Meanwhile the role of IT in the minute-by-minute functioning of our society has greatly increased in recent years. What about hospitals, ports, airports, schools, police stations, and ambulance dispatchers? All of them can only function with working desktop PCs. And those PCs are often running Windows without the latest updates. Criminals or foreign cyber armies can take over these systems, gain a stranglehold on our society and unlike rumbling tanks we would only figure this out after it was already done (or even much later than that).

If cybercrime and even cyber-warfare were really so vitally important, it would be logical for the government to institute a computer education that really teaches, to dismantle of our software monoculture, and reduce our high dependency on foreign service-providers. Real advances in these areas would make so much more sense than abrogating yet more power to a government that displays ever more totalitarian tendencies and, at the same time, highly questionable competence.

Update: While writing this column a criminal (presumed to be from Russia) made my point by infecting 100.000 computers via a Java vulnerability and a hack of the Dutch news website nu.nl around lunchtime. All infected computers ran MS Windows. More details in the post mortem rapport of Fox-IT.[152]

Originally a Webwereld column

9.13 DIY privacy, because the law no longer works

2011

Over the last few years, it seems as though everything that is centralised fails. Governments fail to solve societal problems (or even just complete a successful IT project), central banks fail to monitor the behaviour of ordinary banks, IT companies fail to offer us solutions that are safe and respect our privacy somewhat...

Decentralisation works better: bit-torrent, non-Western popular revolts, open source software, hacktivism and to a certain extent the Occupy movement. I am glad Bits of Freedom and international counterparts such as the EFF exist because they put issues on the agenda that most of the over-50 politicians would not otherwise consider. In Berlin, the Pirate Party has over 9% of the seats in local government and is spreading rapidly across Germany.

Civil liberties evaporating

But is all this really upholding our ‘rights’? Because despite all petitions, motions, actions and other initiatives our (digital) civil liberties are still evaporating. In the Netherlands it is virtually impossible to finish high school without buying Microsoft or Apple products, despite a long string of promises and agreements about this from our government. There are so many PCs that are controlled by cyber criminals that Microsoft had to set up a specific spring-cleaning for the Netherlands without user consent. This also makes it immediately apparent who *really* controls all these systems. Meanwhile, the government uses its own catastrophic Diginotar failure as a pretext for yet more government regulation of the online world.

The way the ACTA treaty brutally sweeps all issues of democratic control off the table, clearly indicates where the interests of our Atlantic partners lie. SOPA is just the cherry on the ice cream to show why we should no longer be dealing with the US-based IT services: Unsuitable (read the article in this book).

Corporate power

It might be a better use of our time just to accept that our government is no (longer?) capable of resisting corporate power. Somehow or other a slow-motion palace revolution has occurred where the government wants to increase 'efficiency' by relying on lots of MBA-speak and corporate management wisdoms that worked so well for the banking sector. The fact that the government's primary function thereby evaporates does not seem to bother it. Meanwhile the companies themselves are apparently too busy making profits and fighting each other to worry about civil rights and other archaic concepts from the second half of the 20th century.

So rather than always trying to influence a system that ignores our interests, we can simply take care of each other and ourselves. This conclusion is not pleasant, but it gives clarity to what we have to do.

DIY – Do It Yourself

One good example is the Bits of Freedom weekly workshops on how to install encryption software and its publications that help people get to grips with these tools. The organisation should use its clout to get the slogan of "Crypto is cool" on everyone's lips. The NLnet Foundation should focus its energies on promoting the hip and user-friendly aspects of these pieces of software. Webwereld journalists should be looking for a modern, technical Deep throat to make 'anonymous-advanced-OV-chip-card-hacking' available to the general public.

Empower yourself

Civil rights organisations and hacktivists can play a very different but probably even more effective role. Since 2006, I have ensured my own email privacy by no longer relying on the law, but by using a server outside the EU, SSL connection to it through a VPN tunnel entering the open internet also outside the EU. And then I encrypt as many emails as possible individually with GPG. I suppose the fact that all those hordes of terrorists (who, our government asserts, are swamping Europe) have no doubt adopted such measures - for less than 20 euros a month – making all the data retention measures a complete and pointless waste of resources.

What is possible now with email will soon be possible with telephony by using VOIP through international VPNs. This will even happen soon with mobiles (although your location information will remain a problem).

Then add an anonymous public transport card hack, a future version of Bitcoin for money transfers, and all you will need is a freshly installed Linux laptop (with an encrypted hard disk[153]) and Bob's your uncle. Just resist the temptation to put your whole life on Facebook and auto-tweet your GPS-data from your phone.

Then you can forget about any digital privacy legislation. You do not need government. You empower yourself as a modern citizen - better living through technology. Too bad it had to come to this – that old democracy concept seemed a really nice idea.

At Cryptoparty.org[154] you can find places where citizens are teaching each other how to use privacy enhancing tools. If your locale is not on the list, then add it and find people to get going where you live!

Originally a Webwereld column

9.14 Cybercrime or the end of scarcity? The future of hacking

2010

On October 14th, The Club of Amsterdam is meeting to discuss 'The future of hacking'.

The term hacking (and hacker) means very different things to different people.

Most will associate the term with computer-enabled crime; from Russian mobsters stealing western credit cards to spammers sending billions of unwanted email advertisements for Viagra to Chinese intelligence employees attempting to break into NATO computers. But for those calling themselves hacker (or being called hackers by their peers), hacking just refers to the creative use of technology, any technology, to do new and unexpected things.

These two very different meaning of the term continue to cause a lot of confusion in any discussion about it. This piece will expand on both the cybercrime and creative technology uses and see where they meet.

Cybercrime and criminals

The term cybercrime itself suggests that computer and the networks that connect them are a new phenomenon in the eyes of law-enforcement and the justice ministry. If a crime is enabled by a telephone or car this is not worthy or separate classification. But if a computer or the internet is involved a crime quickly becomes a ‘cybercrime’. A recent BBC item mentions a big case were 45 million credit cards were stolen. The financial impact of this theft was either not known or not made public.

The trouble with evaluating ‘cyber’-crime is both the scope of the subject and the lack of hard data. From copyright infringement via credit card fraud to child pornography (more accurately imagery of child abuse) cybercrime is a field that encompasses a wide range of activities of varying seriousness and with very different levels of impact on the victims.

Even more troubling is estimating the effectiveness of law enforcement do prevent or these crimes or at least bring to justice the perpetrators after the fact. Can this effectiveness be measured and if we can, is it worth logging everyone’s email and cell phone communications to capture an unspecified number of thieves? Precisely because we lack clear information on both the scale of the problem and the effectiveness of the measures trying to cope with it, there is no way of telling either way.

Happy side of hacking

The much happier side of hacking is all the wonderful things people are doing with technology all over the world, taking it apart and making it do stuff the original designers and producers never imagined. Thanks to intrepid hackers, computers have become utterly commoditised and all of us can be connected to the global Internet for 10 euros per month. This democratisation of technology has spawned not only entire new industries but also new ways for people to communicate, organise and participate in global affairs whoever and wherever you are.

Before computers became small and cheap, people calling themselves hackers were tinkering with all kinds of other hardware. Now computers, sensors and other components have become so cheap hardware hacking is becoming just as democratised as merely using a computer.

The first desktop factories, also known as 3D printers, for home use with use-at-home pricing are a reality today and over the next decade they will develop in the same way our commodore 64 developed into smart-phones and laptops. Cheaper and twice as powerful every 18 months. If we can all print our consumer goods at home, will anyone even want to steal anything? Of course, someone will figure out a way to print an AK-47 (just for fun mind you!) and then things will get really interesting.

Get techno-literate

Everyone having access to technology has both benefits and problems; from YouTube and WikiLeaks as new global media to roadside bombs detonated by cheap mobile phones to surveillance possibilities the Stasi could only dream of. In a world re-defined by technology everybody needs to become a little bit techno-literate. Ignorance of new possibilities will mean losing out on great opportunities for a better life and becoming a victim of those who would use the new tools for criminal or other bad purposes.

Hackers might save the world, especially if every citizen adopts the hacker ethic of collaboration, free sharing of knowledge and an anti-authoritarian attitude to keep would-be stasis at bay.

10.

About my InfoSec Book

Secure communications & computing, what it is, why you need it, how you get it

With journalist Silkie Carlo I have co-authored a 'handbook' on practical information security for journalists commissioned by the UK Centre for Investigative Journalism. The CIJ handbook 'Information Security for Journalists'155 was launched at the CIJ Summer School 2014 in London. Since this book was written post-Snowden – please use the book for detailed instructions on setting up tools for digital self-defence. *Note: It has been updated yearly.*

The handbook explains the need for secure communications for journalists, activists, politicians and anyone else who seeks to change the status-quo in the world somehow and also retain their basic right to privacy.

'Few things are as practical as a good theory'

The primary focus of the document is to provide a practical how-to that helps non-specialists with the installation and daily use of secure computing and communication habits. Because understanding the underlying theory behind the tools will help re-enforce independent secure behaviour, a short introduction to theoretical concepts is included. We urge everyone to spend the time required to read and understand these paragraphs. Most of the readers of this document will have to use the tools without much technical assistance from specialists, so actually understanding what you are doing is vital to doing it right.

Why you need secure communications

If you are trying to push the world in a different direction, the world usually pushes back. The more successful you are, the harder the pushback will be. Over the last decade, the amount of electronic surveillance has increased to levels, especially in western countries, previously only seen in the former East Germany. If you are effective as a journalist, activist or politician who is challenging the-powers-that-be, your communications will be monitored at some point (if you are not being monitored or being arrested every now and then, you are obviously not trying hard enough).

When communicating with others for planning, organisation or just sharing basic info it may be useful to keep what you are sharing, the fact that you are sharing it and with whom you share it hidden from the prying eyes of governments and/or corporations.

The fact that 'you are not doing anything wrong' is irrelevant. Sadly, we have arrived in the phase in history where breaking the law or even being accused of anything specific is no longer a requirement to monitor, imprison or even kill citizens outside the context of due process and a fair trial. The fact that this kind of monitoring may be technically illegal in most western countries is sadly just as irrelevant these days. If it can be technically monitored, it very well might be.

What does secure mean?

When we say secure, we do not mean: ‘Difficult to intercept’ or ‘probably won’t get broken into’. Secure must mean intrinsically secure. Secure must mean it is protected against the strongest possible attack a hyper-power-nation-state-level organisation can mount against it. The security must be derived from basic mathematical concepts that cannot be circumvented by any known method over a time-scale that is relevant (the known remaining life of the planet earth is a good start).

To achieve this it is vital to only use methods and mechanisms that have been tested by as many experts as possible. For practical purposes this means only using Free Software (also known as open source software).

Security, like changing the world, is hard. Getting things working and changing your computer habits will require some effort. If you do not have the time or inclination to make this effort, that’s fine. Just do not assume you can use your computer without informing whomever you may be opposing. Doing everything offline is a perfectly good way of avoiding electronic surveillance, just not practical for everyone.

How to get it

The InfoSec Handbook will focus mostly on setting up a secure system and email as a means for communications and securely sharing information.

Readers, check out Part 2 for the 2020-updated version of Arjen's complete and completely free book.

Endnotes (Part 1)

[1] https://www.youtube.com/watch?v=8rJTJ_wA2NY

[2] Read 'What's it for, the objectives of policies & systems' (chapter 10, Random stuff in this book)

[3] http://www.xs4all.nl/overxs4all/maatschappelijk/downloads/internet_voor_iedereen.pdf

[4] https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/nieuws/burgemeesters-willen-stemmen-met-stemcomputer.5476968.lynkx

[5] http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

[6] https://www.youtube.com/watch?v=B05wPomCjEY

[7] http://wijvertrouwenstemcomputersniet.nl/English

[8] https://en.wikipedia.org/wiki/Voter-verified_paper_audit_trail

[9] US Anti-Counterfeiting Trade Agreement

[10] https://www.youtube.com/watch?v=1p-TV4jaCMk&feature=youtu.be

[11] https://en.wikipedia.org/wiki/United_States_Declaration_of_Independence#Annotated_text_of_the_Declaration

[12] https://news.wisc.edu/was-declaration-of-independence-inspired-by-dutch/

[13] https://sourcebooks.fordham.edu/mod/1581dutch.asp

[14] https://web.archive.org/web/20160614195837/http://webwereld.nl/e-commerce/53881-5-miljoen-nederlanders-downloaden-uit-illegale-bron

[15] Read chapter 6.7 ‘A reasonable discussion’

[16] https://www.techdirt.com/articles/20110603/00214214533/entertainment-industry%20-lawyer-public-domain-goes-against-free-market%20capitalism.shtml

[17] https://vimeo.com/24218524

[18] https://www.lessig.org/

[19] https://craphound.com/

[20] https://www.wired.com/2011/06/internet-a-human-right/

[21] https://torrentfreak.com/anti-piracy-group-stuns-the-world-with-torrent-site-massacre-100715/

[22] https://vimeo.com/12199740

[23] Read chapter 6.7 ‘A reasonable discussion’

[24] https://web.archive.org/web/20160326164439/http://www.engagetv.com/webcast_het_grote_downloaddebat

[25] https://en.wikipedia.org/wiki/Moore%27s_law

[26] https://kodi.tv/

[27] https://reprap.org/wiki/RepRap

[28] https://www.theguardian.com/technology/2010/jun/01/digital-economy-act-will-fail?showallcomments=true

[29] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1436186

[30] https://www.theguardian.com/technology/blog/2010/feb/23/opensource-intellectual-property

[31] http://eyewitnesstohistory.com/louis.htm

[32] https://har2009.org/

[33] https://wilfreddolfsma.net/

[34] https://arstechnica.com/information-technology/2009/07/european-publishers-want-news-access-controls-legislated/

35 https://www.nytimes.com/2004/05/26/world/from-the-editors-the-times-and-iraq.html

36 https://www.reuters.com/article/us-nuclear-iaea-iran-exclusive/no-sign-iran-seeks-nuclear-arms-new-iaea-head-idUSL312024420090703?sp=true

37 https://rop.gonggri.jp/?p=89

38 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1436186

39 https://books.google.co.uk/books?id=cxZp0sV3V80C&dq=inauthor:Lawrence+inauthor:Lessig&hl=en

40 http://www.free-culture.cc/

41 https://gendo.ch/blog/arjen/the-missed-opportunity-of-avoiding-prism

42 https://www.information.dk/udland/2014/01/nsa-spied-against-un-climate-negotiations

43 https://www.reuters.com/article/us-security-snowden-germany/snowden-says-nsa-engages-in-industrial-espionage-tv-idUSBREA0P0DE20140126

44 https://gendo.ch/en/blog/arjen/kerckhoff-lecture-what-europe-needs-to-do-after-snowden

45 https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN#title2

46 https://en.wikipedia.org/wiki/United_States_v._Microsoft_Corp.#Judgment

47 https://en.wikipedia.org/wiki/Microsoft_Corp._v._Commission#Judgement

48 https://www.raspberrypi.org/

49 https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

50 https://tails.boum.org/

51 https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/dutch-fund-improvement-apa

52 https://www.techrepublic.com/article/how-munich-rejected-steve-ballmer-and-kicked-microsoft-out-of-the-city/

53 https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/french-gendarmerie-open-sou

54 https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/spains-extremadura-starts-sw

55 https://www.governmentcomputing.com/news/

56 Read chapter 8.3 'Doublethink and Zen', chapter 9.12 'Cybercrime; prevention versus repression', chapter 8.5 'Docter, docter...', chapter 7.7 'Asbestos is also useful', chapter 7.6 'Unsuitable', chapter 7.5 'Waiting for the big one', chapter 9.13 'DIY privacy, because the law no longer works', chapter 7.10 'Autoimmune disease in the pig pen'

57 https://www.youtube.com/watch?v=sKOk4Y4inVY

58 https://www.youtube.com/watch?v=L_YBplucfuk

59 Electronic Health Records

60 NOiV is a project that aims to promote the development and the use of open standards and open source software within the Dutch government.

61 https://www.theguardian.com/technology/2012/may/14/problem-nerd-politics

62 https://www.youtube.com/watch?v=HlZRcxvGIWE

63 https://www.justice.gov/atr/us-v-microsoft-proposed-findings-fact-0

[64] https://boingboing.net/2011/02/17/dhs-erroneously-seiz.html

[65] https://web.archive.org/web/20160305100231/http://www.theguardian.com/technology/2011/jul/03/us-anti-piracy-extradition-prosecution

[66] https://www.nic.ch/

[67] https://wikileaks.org/ and https://wikileaks.ch/

[68] https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[69] Read chapter 7.10 ‘Autoimmune disease in the pig pen’

[70] https://www.fsf.org/

[71] https://www.youtube.com/watch?v=QOEMv0S8AcA

[72] http://cryptome.org/cyberinsecurity.htm

[73] https://www.theregister.co.uk/2010/04/23/nhs_worm_infection/

[74] https://www.ccc.de/updates/2008/schaubles-finger?language=en

[75] https://web.archive.org/web/20160409015444/http://downingstreetmemo.com/memos.html

[76] https://gnupg.org/

[77] https://www.schneier.com/blog/archives/2008/01/dutch_rfid_tran.html

[78] https://www.computerweekly.com/blog/Public-Sector-IT/Open-standards-Youll-know-one-when-you-see-one-says-Microsoft

[79] Read chapter 8.3: ‘Doublethink and Zen’

[80] https://freesnowden.is/

[81] https://web.archive.org/web/20161119021458/http:/gendo.nl/en/blog/arjen/the-other-it-from-another-europe

[82] http://europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN#title2

[83] https://cyber-rights.org/interception/stoa/interception_capabilities_2000.htm

[84] https://www.justice.gov/atr/us-v-microsoft-proposed-findings-fact-0

[85] https://boingboing.net/2011/02/17/dhs-erroneously-seiz.html

[86] https://en.wikipedia.org/wiki/Magna_Carta

[87] https://ripe65.ripe.net/

[88] https://www.huffingtonpost.co.uk/2012/10/31/police-powers-snoop-hackers_n_2051713.html?guccounter=1 (mind you: cooookies)

[89] https://www.wired.com/2012/11/russia-surveillance/

[90] https://web.archive.org/web/20160403085744/http://files.gendo.nl/media/This_is_Hell_radio_20130622.mp3

[91] https://en.wikipedia.org/wiki/Doublethink#Origin_and_concepts

[92] https://web.archive.org/web/20160404111747/http://www.gendo.nl/en/blog/arjen-int/desktop-mono-culture-for-the-dutch

[93] https://joinup.ec.europa.eu/collection/open-source-observatory-osor

[94] https://www.wired.com/2007/08/microsoft-allegedly-bullies-and-bribes-to-make-office-an-international-standard/

[95] http://www.cptech.org/ms/harm.html

[96] https://users.dcc.uchile.cl/~fhoffa/peru2ms/

[97] https://cis-india.org/openness/blog-old/an-interview-with-arjen-kamphuis

[98] https://www.ams-ix.net/ams

[99] https://www.suares.com/

[100] https://en.wikipedia.org/wiki/Auguste_Kerckhoffs

101 https://gendo.ch/en/blog/arjen/the-missed-opportunity-of-avoiding-prism

102 https://projekte.sueddeutsche.de/artikel/digital/sz-international-e366019/

103 https://files.gendo.ch/presentaties/Gendo_Kerckhoffs_13-06-2014_Final.pdf

104 https://en.wikipedia.org/wiki/Daniel_Ellsberg

105 https://en.wikipedia.org/wiki/Mike_Gravel

106 https://en.wikipedia.org/wiki/Filibuster

107 https://collateralmurder.wikileaks.org/

108 http://www.usf-iraq.com/?option=com_content&task=view&id=12818&Itemid=128

109 https://web.archive.org/web/20130213175041/http://downingstreetmemo.com/memos.html

110 https://web.archive.org/web/20130305233149/http://www.cageprisoners.com/

111 https://anniemachon.ch/annie_machon/2008/05/british-spies-a-1.html

112 https://file.wikileaks.org/file/cia-afghanistan.pdf

113 https://web.archive.org/web/20100410170305/http:/www.usf-iraq.com/?option=com_content&task=view&id=12818&Itemid=128

114 https://www.justforeignpolicy.org/iraq-afghanistan-a-promise-kept-a-promise-deferred/

115 https://www.youtube.com/watch?v=5rXPrfnU3G0

116 https://www.youtube.com/watch?v=is9sxRfU-ik

117 https://web.archive.org/web/20130123161055/http://atwar.blogs.nytimes.com/2010/04/07/reaction-on-military-blogs-to-the-wikileaks-video/

118 https://web.archive.org/web/20120118104321/http://archive.truthout.org/iraq-war-vet-we-were-told-just-shoot-people-and-officers-would-take-care-us58378

119 https://web.archive.org/web/20120211100032/http://www.downingstreetmemo.com/

120 https://web.archive.org/web/20120512122327/http://mirror.wikileaks.info/leak/cia-afghanistan.pdf

121 https://en.wikipedia.org/wiki/Granai_airstrike

122 https://www.youtube.com/watch?v=RJ194S7KjRg and https://thedaywefightback.org/

123 https://en.wikipedia.org/wiki/Churchill#.22We_shall_never_surrender.22

124 https://donate.torproject.org/

125 https://tails.boum.org/contribute/index.en.html

126 https://www.fsf.org/

127 https://www.un.org/en/universal-declaration-human-rights/index.html

128 https://www.youtube.com/watch?v=PY2RaDwsLWk&feature=youtu.be&t=18m4s (London Real)

129 Read chapter 8.2 'The missed opportunity of avoiding PRISM', chapter 9.11 'Privacy a decade on' and chapter 9.13 'DIY privacy, because the law no longer works'

130 https://20committee.com/2013/09/04/snowden-nsa-and-counterintelligence/

131 https://web.archive.org/web/20161118130628/http:/nos.nl/

132 https://web.archive.org/web/20161118130628/http:/sandervenema.ch/2013/08/speaking-truth-to-power/

133 https://archive.nytimes.com/www.nytimes.com/ref/international/middleeast/20040526CRITIQUE.html?_r=0

134 https://www.theguardian.com/world/2013/may/26/iceland-crackdown-internet-porn

135 https://www.theguardian.com/commentisfree/2013/jan/27/obama-war-on-whistleblowers-purpose

136 https://whowhatwhy.org/2012/09/27/the-complete-idiots-guide-to-iran-and-the-bomb-or-how-i-learned-to-stop-worrying-and-love-the-facts/

137 https://www.youtube.com/watch?v=8uFJpq26dHI

138 https://in.reuters.com/article/nuclear-iran-iaea/iran-move-to-speed-up-nuclear-programme-troubles-west-idINDEE91L00P20130222

139 https://en.wikipedia.org/wiki/1953_Iranian_coup_d%27%C3%A9tat#US_role

140 https://whowhatwhy.org/2012/09/27/the-complete-idiots-guide-to-iran-and-the-bomb-or-how-i-learned-to-stop-worrying-and-love-the-facts/

141 https://www.wired.com/2013/03/stuxnet-act-of-force/

142 https://en.wikipedia.org/wiki/Sam_Adams_Award

143 https://www.youtube.com/watch?v=d36xEvVnF2I&feature=youtu.be

144 https://www.youtube.com/watch?v=4vQNWYnQjUE

145 https://www.youtube.com/watch?v=x1r7-ralebI

146 https://therealnews.com/

147 http://europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN#title2

148 https://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm

149 https://www.huffingtonpost.co.uk/2012/10/31/police-powers-snoop-hackers_n_2051713.html

150 https://www.wired.com/2012/11/russia-surveillance/

151 https://vovklict.nl/intercom/2010/3/33__38.pdf

152 https://blog.fox-it.com/2012/03/16/post-mortem-report-on-the-sinowallnu-nl-incident/

153 https://www.veracrypt.fr/en/Home.html

154 https://www.cryptoparty.in/

155 https://www.journalism.co.uk/news/information-security-for-journalists-/s2/a562525/

Part II:

The InfoSec Book

PRESS
I'M WITH WIKILEAKS
NATIONAL SECURITY AGENCY
MONITORED DEVICE
ΜΟΛΩΝ ΛΑΒΕ

Information Security for investigative journalists

This handbook is a very important practical tool for journalists. And it is of particular importance to investigative reporters. Since the revelations of Snowden in 2013, journalists are aware that virtually every electronic communication we make or receive is being recorded, stored and subject to analysis. As this surveillance is being conducted in secret, without scrutiny, transparency or any realistic form of accountability, our sources, our stories and our professional work itself is under threat. In addition more and more governments make a disconcerting departure from legal principles of source protection in favour of unbridled spying powers.

This document explains the need for secure communications for journalists, activists, politicians and anyone else who seeks to change the status-quo in the world somehow and also retain their basic right to privacy.

After Snowden's disclosures we also know that there are real protective measures available. The 2014 handbook Information Security For Journalists from the CIJ was the first to lay out the most effective means of keeping your work private and safe from spying. It explains how to write safely, how to think about security and how to safely receive, store and send information that a government or powerful corporation may be keen for you not to know, to have or to share. To ensure your privacy and the safety of your sources, Information Security For Journalists will help you to make your communications indecipherable, untraceable and anonymous.

Although this handbook is largely about how to use your computer, you don't need to have a computer science degree to use it. Its authors Silkie Carlo and Arjen Kamphuis and the experts advising the project, are ensuring its practical accuracy and usability, and work with the latest technology.

Based on Gavin MacFadyen's intro in the original book from 2014 (when he was Director of the Centre for Investigative Journalism)

Free download

This handbook is, in the tradition of Silkie and Arjen, offered as a free download. If you think the book is of use to you, please consider a donation[1] to the Centre for Investigative Journalism (CIJ, UK), the Dutcht NVJ (Nederlandse Vereniging voor Journalisten) or the Dutch VVOJ (Vereniging van Onderzoekjournalisten).

January 2020

[1] *http://tcij.org/donate*

Acknowledgements

I would like to express my deep gratitude to Arjen Kamphuis for his patient and generous teaching.

Many thanks to Gavin MacFadyen and the CIJ for commissioning and trusting us with the responsibility of writing a handbook that aims to protect his journalists and their sources, and for his information security advocacy generally.

We collectively thank the whistleblowers and hacktivists, none more than Edward Snowden, for democratising the information that we now profit from in defending ourselves, our sources, and a free press. With solidarity and gratitude to the journalists who intend to use this manual,

Silkie Carlo, 2016

Thanks to the heroes of the Free Software Foundation who foresaw the problems we now have 30 years ago and moved to make sure we have alternatives.

Thanks to the developers and hackers who freely share their work with all humanity.

Thanks to Gavin, Juliet and Minal at CIJ for all their great work in support of journalism (including supporting us in making this book).

Thanks to the whistleblowers for their courage and sacrifice.

And thanks to Silkie Carlo, my co-author, for curiosity, drive, grace under fire and never settling for less than her best.

I dedicate this book to my parents, Ida & Andre Kamphuis, who raised me to stand up for principles and never bow down to authorities trying to destroy them.

Arjen Kamphuis, 2017

Preface

With journalist Silkie Carlo[2] I have co-authored a 'handbook' on practical information security for journalists commissioned by the UK Centre for Investigative Journalism[3]. The CIJ handbook 'Information Security for Journalists[4]' was launched at the CIJ Summer School 2014[5] in London. The book will be forever freely available in a range of electronic formats..

Although this book was originally written for investigative journalists most of the described concepts and technical solutions are just as usable by lawyers or advisors protecting communications with their clients, doctors protecting medical privacy and of course politicians, activists or anyone else who engages powerful state and corporate organisations. Really, we're all journalists now.

If you have reasons to suspect your online movements are already under some form of surveilance you should not download this book using a computer or netwpork associated with your identity (such as your home or work systems).

[2] *http://silkiecarlo.com/*

[3] *http://www.tcij.org/*

[4] *http://www.tcij.org/resources/handbooks/infosec*

[5] *http://www.tcij.org/summer-school*

In the 12 months after Snowdens revelations, all the most extreme paranoid fears of privacy activists and information security experts have turned out to be but cuddly little problems compared to the reality of industrialised espionage on the entire planet. Anyone who has kept abreast of the ongoing revelations as a journalist with the desire to protect their sources and their stories from government or corporate snoopers may have felt despair. Is everything with a chip and a battery spying on us? When considering most off-the-shelf computing devices such as laptops, tablets and smartphones, the situation is indeed dire. But there are steps you can take and those steps are not expensive nor do they require a PhD in computer science. Using a computer system that can withstand all but the most advanced attacks by the most advanced nation state-level attackers is well within the reach of everyone.

That is, anyone who is willing to spend a few days learning to use software that is free of cost and hardware that is already available to you or that can be bought for under £200. This handbook can get you started on understanding how to secure your data and communications and those of your sources, and to use tools and methods that have been proven to work in the most extreme situations by experts all over the world.

Depending on your pre-existing computer skills this may be a bit of a learning experience, but trust that many have gone before you who also did not consider themselves experts and yet they managed to become comfortable with the concepts and tools described in this book.

If you are a journalist in the 21 st century, you need these tools. After all, William Randolph Hearst said decades ago: journalism is writing down what powerful people and institutions do not want written. If you don't consider yourself to be a journalist but merely insist on actually having the right to privacy guaranteed to you under the UN Declaration Of Human Rights [1948] Article 12 - this book is for you too.

Like almost everyone who ever created anything, we could only do so by standing on the shoulders of a thousand generations that came before us. Thus, this book will be forever freely available in a range of electronic formats without any restrictions. If the format you would like is missing, just let us know.

If you appreciate this work, please spread it around as much as possible and help us make the next version better. Constructive feedback of any kind is most welcome. The problem will keep developing and so will our response. Please contribute to sharing this knowledge and promoting these tools in any way you can.

Arjen Kamphuis

Introduction

Imagine opening your inbox to find an anonymous email from someone offering to share important, sensitive documents of international significance with you. The source, and the information, requires the highest level of protection. What do you do?

This manual is designed to instruct journalists and media organisations on how to practise information security in the digital age, protecting your work, your sources, and your communications at a variety of risk levels.

Information security, or 'InfoSec', is the practice of defending information from unauthorised access. The information at stake may include a news report you are working on and any associated files, the identity of your source(s), your communication with them, and at times, your own identity.

You don't need to be an I.T. expert to practise InfoSec (although you will certainly learn a lot as you go along!). Using this manual, you could learn to send encrypted emails and documents from your own highly secure laptop within days!

Who Poses a Threat?

Targeted threats

The Snowden revelations exposed the extraordinary abilities of certain government intelligence agencies to intercept communications and gain unauthorised access to data on almost any personal computer or electronic communication device in the world. This could pose an information security risk to investigative journalists working on stories concerning the interests of those governments, their agencies, and their private intelligence contractors.

Many states lack these sophisticated surveillance technologies – but all states do possess surveillance capabilities, some of which can be, and at times have been, used against journalists, with potentially severe consequences. Ethiopia, a less technologically advanced state, is alleged to have launched remote attacks against journalists stationed in US offices.

In the globalised age, some transnational corporations have greater wealth and power than many sovereign nation states. Correspondingly, some transnational corporations possess greater 'security' or surveillance capabilities than many nation states.

It is not only corporations, but sophisticated criminal organisations that have also been known to employ impressive surveillance technologies – and some criminal organisations may overlap with criminal elements in government. The Mexican army spent $350 million on surveillance tools between 2011-2012, and reportedly now possess technologies to collect text messages, phone calls and emails; to remotely automate audio recording on mobile phones; and even to detect movement through walls using radar technology. Also between 2011-2012, nine journalists were killed in Mexico in association with their work.

Unauthorised access to your data may entail its use, disclosure, disruption, modification, inspection, recording or destruction. You and your source could invoke legal or physical risks, and the information at the heart of your story could be compromised. In high-risk situations, InfoSec may be as important as wearing a bulletproof vest and travelling with bodyguards. However, because digital threats are invisible, complex and often undetectable they can be underestimated or overlooked.

Dragnet threats

You may also wish to protect yourself from 'dragnet' surveillance programs, led by the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ).

These are programs that collect and sometimes analyse the world's online and telecommunication data - potentially enabling retroactive investigation. Even police forces in the UK have accessed stored communications data to identify hundreds of journalistic sources.1

Practising InfoSec

As an effective journalist, you will find yourself disturbing a few hornets' nests in the course of your career. Therefore, practising good InfoSec means normalising several permanent strategies that easily fit into your everyday work. It also means employing case-by-case protection strategies, as you will need to use stronger and more effortful InfoSec methods when working on sensitive topics, and with vulnerable sources.

The first step to practising good InfoSec is to be aware of the threats; the second is to be aware of your hardware and software vulnerabilities. Understanding how and why unauthorised access happens is the first step in learning how to protect yourself from it.

Legalities

Despite the fact that the pervasive surveillance of law-abiding citizens almost certainly contravenes international human rights laws, use of certain privacy tools can be illegal.

Several of the privacy tools discussed in this handbook are cryptographic tools. This cryptography may be illegal, or require a license, in several countries including China, Cuba, Iran, Libya, Malaysia, North Korea, Singapore, Sudan, and Syria. When entering some of these countries, you may need to declare any IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources, 4 February 2015 encryption technology on your laptop. You should consider the legal implications of using cryptography and make informed decisions about where and when it is safe for you to do so. You can find out more about cryptography laws for each country here: http://www.cryptolaw.org

Threat modeling

There is a lot of information in this handbook about various possible threats, and measures that can be taken to defend against them. However, since attack technologies are always changing and much of their use is entirely secret, we rarely confidently know the exact threats; when, where and to whom they apply; or the efficacy of our defenses.

Therefore, it is down to you to perform a personal risk assessment and design an appropriate defensive response during the course of reading this book. You may also want to factor in practicalities – some users may compromise their InfoSec, whilst aware of the risks, to meet other practical demands in their work, whereas some users practice sophisticated InfoSec above their perceived need because they find it practically doable.

Some basic questions you may wish to ask yourself when threat modeling for your InfoSec strategies are:

1. Who could your adversaries or potential attackers be?
2. What tools might your potential attackers possess?
3. How likely is your potential attacker to use their available tools against you?
4. What risks could arise, for you and those you communicate/work with, from a targeted attack?

5. What risks arise from passive surveillance? How extensive are the tools used in passive surveillance?
6. What defence strategies are practical, safe, and effective in light of your evaluated risks?
7. What defence strategies are practical, safe, effective, and instructible for my sources and colleagues, in light of their evaluated risks and/or the risks incurred by our communication?

The threats will change, with time – but so too will the technologies available to protect journalists and citizens. So, it is important to understand InfoSec in theory, and to always continue learning about InfoSec in practice.

1.

Protecting the System

Your security and/or encryption methods will only be effective if each level of your system is secure. You can send your emails with unbreakable encryption, or use the strongest conceivable passwords, but if your system is hacked, or otherwise vulnerable, your efforts may be futile, as your encryption can be circumvented without any need to break it.

Depending on your risk level and the sophistication of your adversary, protection strategies range from simply keeping your laptop or phone on you at all times, to using a second-hand, cash-bought, laptop and practising robust InfoSec, during a specific project.

Think of 'protecting your system' as building a house of cards – for it to work, you must build your security from the bottom up.

In this chapter, you will learn how to build the foundations of a secure system by managing the security of your hardware and firmware.

This chapter is the most important of the book. It is also fairly technical, and contains the most challenging information of any chapter in the book. The solutions here are many, but ultimate security is the outcome of only one. Here, we lay out the horrible reality of the extent of hardware vulnerabilities, and leave you to decide what the appropriate security measures are for yourself. For several of the solutions described here (such as specialist modifications to hardware, and the replacement of firmware) you will need expert help.

As lengthy and technical as much of this chapter is, please do read on! You should be aware of the vulnerabilities within your own system, even if you do not have the ability or need to currently solve them. This is important information that will guide your trust and use of your system, and prepare you for the future, simpler solutions that we hope will soon be developed.

1.1 Your computer model

Definitions

- **Interface –** screen
- **Applications –** your software/programs
- **Middleware -** programming that 'glues together'/mediates between two separate and often already existing programs: e.g. allows programs to access databases
- **Operating System –** Windows XP/7/8/10, Mac OS X, Linux, etc.
- **Firmware –** fundamental software programmed onto hardware that provides instructions for how the device communicates with the other computer hardware
- **Hardware –** the physical elements that comprise a computer system

In this chapter, we will primarily consider security at the most fundamental level: hardware and firmware.

1.2 Hardware and firmware

'Hardware' refers to your physical machine. Desktop computers are not recommended for important journalistic work as they are immobile and as such not only impractical, but vulnerable to physical intervention when you are not around. Laptops will be discussed here.

For our purposes, 'laptop' refers to all physical components, including the battery, hard disk drive, CD drive, Wi-Fi card, microphone, and webcam. Let's also consider additional hardware: any keyboard, mouse, scanner/printer, webcam, and so on that you connect to your laptop.

Threats to hardware may be:

- Theft or damage
- Physical attack
- Virtual/remote attack

The main risks to your hardware are that it will be stolen, damaged, physically tampered with or 'bugged'; or virtually/remotely accessed in order to transmit signals (i.e. collect and deposit your information).

1.3 Hardware protection

Five key measures are important for hardware protection:

Preventing virtual and physical attacks on your hardware

- Buying the right laptop
- Modifying your hardware

Preventing physical attacks on your hardware

- Buying your laptop anonymously
- Guarding your laptop
- Detectability measures (should you be separated from your laptop/s)

Although these five steps may sound confusing and even daunting at first, they are all entirely doable for journalists who are new to I.T. and InfoSec. How to obtain and maintain your secure hardware is explained in this chapter – all you have to do is choose the risk level you want to prepare yourself for, and take the appropriate steps.

1.4 Preventing virtual and physical attacks on your hardware

1.4.1 Buying the right laptop

What laptop you buy determines the security level you will be able to achieve. As we learn more about extensive surveillance capabilities from the Snowden documents, we learn too what machines are and are not securable. Hopefully, with time, we will be able to develop more secure solutions. However, at the moment, very few laptops are entirely securable against the greatest threats.

This may not be a problem for you or your source, depending on who your adversary is. If you are defending your communications and data from a powerful government or an ally (which, in practical terms, may include significant banks and corporations), you will need excellent security for your laptop/s. Otherwise, whether you are defending against corporations, political, military, terrorist or rebel groups, private security firms, or specific individuals, you will have to estimate how sophisticated the tools of your adversary are; how easy those tools would be to employ against you; how important you are as a target; and thus, what measures you wish to take.

There are four issues to consider when buying a laptop that determine the securability of your system.

Hardware maintenance

You may wish to have a laptop that allows you to unscrew the casing and get inside the machine, so you can do some basic hardware 'maintenance', and choose which components to keep or disable. Many IBM/Lenovo, HP, and Dell laptops are suitable for this, and provide extensive hardware documentation on their websites that assists with DIY hardware modification2.

You cannot easily open the casing of MacBooks – this requires some skill and even so, performing your own hardware maintenance on a MacBook may void its warranty.

Firmware

Firmware is the software programmed onto your laptop's hardware at a deep, foundational level. In basic terms, firmware provides instructions for how parts of your laptop should communicate with each other. Firmware is another possible attack point, as highly sophisticated hackers (likely state-level) may be able to remotely access it and gain privileged control over your machine. This could undermine your subsequent security efforts.

You can 'lock' your firmware on a MacBook, making your firmware accessible only via a password that you set for it. The ability to lock firmware on a Mac provides a specific security advantage over other laptops, of which only a limited number of models can be secured by the highly technical, specialist task of replacing closed source firmware (whereby the code is privately owned and not publicly available or auditable) with open source firmware (called 'Coreboot'[6], which is free to all and has publicly available and auditable code). Of course, confidence in the security provided by the MacBook 'lock' depends on one's trust for Apple. Likewise, confidence in Coreboot depends on one's trust for the auditors of the code. However, the

[6] *Such hardware flexibility and documentation is also available for other brands – the above suggestions are not endorsements of these brands or their products*

Mac firmware lock has no known vulnerabilities, and using it could make a hack more effortful.

The Mac Firmware Lock: this is such an easy function to use on Mac, and one that provides considerable defence against firmware hacks. Therefore, Mac users at various risk levels may wish to use this.

To set a firmware lock on your Mac (OS X), boot the machine up, holding down 'cmd' and 'R' keys as it boots to enter Recovery mode. On the top menu bar, go to 'Utilities' > 'Firmware Password Utility' > 'Turn On Firmware Password'. Choose a strong password (see chapter 8) and click 'Set Password'. It is very important that you remember this password, or you may lose access to your Mac.

Chipsets

From around 2006, Intel started putting special components in their chipsets (combinations of chips that work together on laptop motherboards) to allow the automated management of systems over a network. This is called 'Intel Active Management Technology', and means that an I.T. technician in a large office/university I.T. suite can update software, or do other things to machines, without having to be physically near them. The problem, of course, is that the same functionality can be abused to install spyware or manipulate the systems in other ways. All laptops made after 2008 contain these chipsets, and are therefore vulnerable to these types of attacks when they are on a network.

The ‘Intel 945’ chipset is the most recently made chipset without this automatable feature, and hence lends itself to a securable motherboard/computer. When choosing a laptop, you can see what its chipset is on the specification.

Operating system

You may also wish to buy a laptop that allows you to install the operating system of your choice (ideally, open source, whereby the source code is publicly available). You can do this fairly easily on most laptops, except MacBooks, where it is a bit more tricky.

You can either totally wipe a pre-installed operating system and install a new one, or you can use ‘virtual machines’ or ‘sandboxes’ on your pre-installed operating system, essentially running multiple operating systems at once. Proprietary operating systems (Windows, Mac) are closed source and may have various inbuilt security backdoors, intentional or otherwise – so it is not known how much security simultaneously running alternate operating systems actually provides. Whilst most laptops allow users to easily wipe their Windows operating system, wiping a MacBook of its operating system is inadvisable as it may compromise the system’s overall functioning.

It is possible to use various operating systems on Mac, but this requires knowledge of how to run a ‘virtual machine’,, which we won’t go into here for the reasons set out above. Alternatively, you can use the operating system Tails on a Mac, which bypasses the hard drive and runs from a USB drive (see Chapter 2).

How can you interpret these four fundamental security issues for your own threat modelling? Remote hardware, firmware and chipset accessibilities are likely to be possible only by the intelligence agencies of technologically advanced and wealthy nations – but all technology tends to be democratised to less powerful groups over time. Therefore, if could potentially list such an intelligence agency as an adversary, you may wish to consider those three vulnerability factors. Even if you do not face such a risk level, you may wish to take some security precautions as a safe measure nevertheless (particularly those that require little effort, such as locking firmware on a Mac).

It is likely that technologically advanced intelligence agencies have access to backdoors in operating systems. However, it may also be the case that especially large or powerful corporations can obtain such knowledge or access too – so if your adversary is a corporate giant, you should consider the security implications of your operating system.

Choosing what laptop to use is not easy – you should take your time processing this information, assessing your risk levels, and deciding how much effort and discipline you will invest into your information security.

Risk level suggestions

Here are some suggestions of what laptops you could buy at various generalized risk levels:

- **Low risk:** *dragnet surveillance, low grade individual hacking, theft*

  You can start with any laptop. A good investigative journalist will outgrow this category before long! Most systems are fairly securable against unsophisticated threats at the software level. By keeping your machine on you at all times, you can defend against theft or physical interventions. You can also avoid the digital dragnet through software and application choices.

- **Medium risk:** *targeted surveillance, by an adversary who is prepared or able to invest relatively limited resources*

  Use either a laptop on which you can wipe the current operating system and install your own (ideally, an open source Linux operating system); or use the Tails operating system for project work from any computer. See chapter 2 for more information on operating systems.

- **High risk:** *targeted surveillance by an intelligence agency*

  There are only a handful of machines that can be confidently secured against remote hardware, firmware and chipset accessibility. Currently, the model that is being most frequently secured in this way is the IBM ThinkPad X60 (and X60s). It has an Intel 945 chipset (i.e.

pre-AMT), and specialist work can be done to secure the hardware and firmware (the proprietary firmware can be replaced by open source firmware, 'coreboot'). You should then use the Tails operating system (see chapter 2) on this secure machine, to maintain system security.

If you require one of these secure machines, please safely make contact with us at the Centre for Investigative Journalism. You can send an encrypted email to infosec@tcij.org or contact the office (http://www.tcij.org/about-cij/contact-cij).

If you want to do-it-yourself, you could buy a laptop with a pre-AMT chipset that allows you to open the casing, and use online documentation for the laptop to guide you through some basic hardware maintenance. For instance, you could remove your laptop's hard disk drive, and remove/disable your laptop's microphone, webcam, Wi-Fi card, Bluetooth card, or 3G modem, and Ethernet port (see point 2 in this chapter). However, unless you have been specifically trained, you will be unable to do the more minute hardware modifications for top security, or to replace the firmware.

- **Top risk level:** *targeted, directed surveillance by an intelligence agency*

In very high-risk situations, you should have at least two laptops that have all the above security measures implemented – only, one of those laptops must never connect to the internet by any means. This will be your 'airgapped' machine – a laptop that never, ever goes online. This can be a very useful machine for storing or accessing files (for example, that you may have on a USB stick), writing articles, and producing your reports on. You, or the specialist helping you, should remove or disable all of the laptop's connectivity devices, to ensure it is truly offline at all times (see point 2). Ideally, both your airgapped and your online machine should be two specially secured IBM ThinkPad X60s.

Fact: Glenn Greenwald uses an airgapped laptop to work on the Snowden documents.

The airgap adds an extra level of security to your/your source's data, because your important documents are stored not only on a secure machine, but also entirely offline. Even the most secure machine may be exposed to some degree of risk when it goes online – particularly if the user is the subject of a directed attack.

1.4.2 Modifying your hardware

Let's take a look at all of the modifiable internal components that could potentially be used to surveil you, your source and your work.

- Webcam
- Microphone
- Hard disk drive
- Wi-Fi card
- Bluetooth card
- 3G modem
- Ethernet port

Webcam

Not only can webcams be remotely and covertly activated for specific targets, but webcam images have also been intercepted as part of dragnet surveillance programs (see the Snowden revelation of GCHQ's OPTIC NERVE program[7]). A simple solution is to place a sticker over your webcam.

Microphone

Your laptop's microphone can also be remotely and covertly activated, to capture audio. You could try putting hot glue over the microphone input on your laptop casing, to muffle sounds. Better still, open your casing and cut the microphone wire.

Hard disk drive

Some hard disk drives have been found to contain 'bad' firmware – that is, they could potentially be activated to compromise your security, should you become a target to an agency with a very sophisticated toolkit.

At high-risk levels, it is advisable to remove the hard disk drive and instead work from USB drives. USB drives are also ideal for storing the highly secure operating system, Tails (see chapter 2) – that is, they can hold a small, anonymising system for you to work from. USB sticks are highly

[7] *http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo*

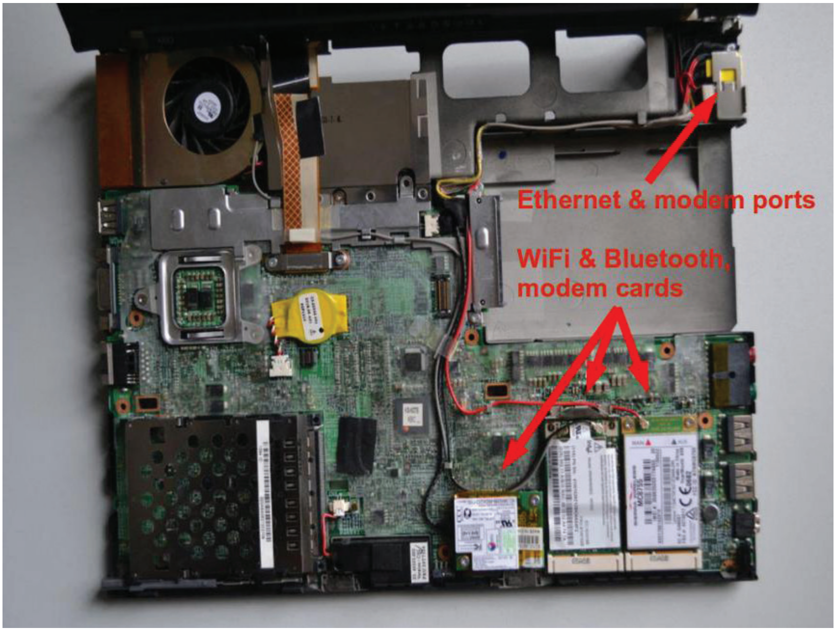
portable, replicable (to share with colleagues/sources), and are easily protectable by high-grade encryption (see chapter 4). This also means that, if your laptop is stolen or damaged, the data stored on your USB is still safe. However, you may wish to keep the hard disk drive for your general day-to-day work, and work from USB drives or Tails sticks for specific projects.

Wi-Fi card, Bluetooth card, 3G modem

At high-risk levels, any element that permits connectivity could be remotely and covertly activated to install surveillance tools, or indeed to send your data back to an adversary. Therefore, you should aim to have as much control over your laptop's connectivity as possible.

The best way to do this is to physically remove connectivity components. This means opening the laptop casing, and unscrewing the Wi-Fi card, as well as any Bluetooth card and 3G modem if your laptop has these (consult your laptop's handbook if you are unsure – copies can often be found online). This may feel like a daunting task at first, but anyone with a steady hand and correct instruction can easily do this first-time.

Then you can control when you are online and offline. You could buy a Wi-Fi USB adapter, which functions in the same way as your Wi-Fi card – it allows you to connect to the internet. The difference is, that you can easily connect and disconnect the adapter from the USB port, and so you decide when you go online and offline. Alternatively, you could choose when to go online via an Ethernet cable.



Ethernet port

The Ethernet port is what you use to physically connect to a ‘local area network’ (LAN), which can be the anything from a network in a large office building or a home router box from your internet provider. Of course, Wi-Fi is now much more commonly used than wired Ethernet connections.

It is known that Ethernet ports have specific security vulnerabilities that can be exploited against especially high-risk targets. If you wish to defend your machine against Ethernet exploitation (e.g. for an airgapped machine), you could fill the port with hot glue. Alternatively, you could disconnect the port wiring inside the laptop.

1.5 Preventing physical attacks on your hardware

1.5.1 Buying your laptop anonymously

As you learn about InfoSec, you may wish to purchase one or two new laptops. This is not only a wise decision when working with a new high-risk source, or when working on a very sensitive project, but to prepare yourself for the possibility of such eventualities, and to implement your new InfoSec learning.

The process of buying secure laptops should be as anonymous as possible in high-risk situations to prevent an adversary from pre-positioning surveillance tools in your hardware; being alerted to your new hardware and thus being motivated to physically or virtually invade your machine after purchase; or tracing your laptop/data back to you and/or your source.

If you are working with a high-risk source, such as an intelligence whistleblower, that person may already be under surveillance. You should assume that the surveillance risk that applies to your source could also apply to you.

The Snowden documents revealed that intelligence agencies intercept devices such as laptops, phones and other electronics, to implant surveillance tools before factory sealing them and putting them back into transit – so you should avoid purchasing any hardware (even chargers) online. Most elements of hardware can be modified to act as surveillance tools.

You should decide what model of laptop you want to buy first (after reading this chapter), and be sure to do any research before buying using the anonymous Tor browser (see chapter 3). To be safe, you can buy your laptop/s in person, with cash. If you are buying an older model you may wish to find an area, preferably some distance from where you normally shop, with several second hand electronics shops. At higher risk levels, you may wish to use several different shops to buy each laptop and accessory (e.g. USB sticks), and whilst shopping, place any device that could track you (i.e. your phone) in a Faraday cage (a metallic enclosure that prevents signal transmission) or leave it somewhere safe at home.

For media and campaign organisations, it is a good idea to pre-emptively tool up with pre-prepared secure equipment (that should be stored in a safe until use) and to train several employees in how to use it. For advice on ready-made toolkits and training, contact infosec@tcij.org.

1.5.2 Guarding your laptop

Preventing theft, damage (intentional or not), and physical attacks on your hardware, if you deem yourself to be at risk of targeted surveillance, means adopting an important new behaviour: keeping your laptop on you, near you, or within your sight at all times. Adopting such behaviour is sometimes called ‘OpSec’, or ‘Operational Security’. If at any point your laptop is left unattended (for example, at home, in a café, or at the office) or is in someone else’s possession (for example, checked-in baggage on a flight; or being held by the police/authorities), you should consider, depending on your risk level, the possibility that the system may no longer be secure.

Keep your secure system as simple, small, and light as possible – avoid connecting the laptop with a mouse, keyboard, printer, docking station, or other devices (which, for high-risk targets, could conceivably be 'bugged') to limit the hardware you need to carry with you or be responsible for.

You need to consider the physical security of your hardware not only presently and in the future, but also retrospectively. Could it have been physically attacked before? How was it manufactured – could the hardware already be compromised?

Since we know that shipment may be a risk, we discussed buying new hardware in person, with cash (point 3). Not only is this a more anonymous way of acquiring a new laptop, but you can take physical responsibility for it immediately.

1.5.3 Detectability measures

Detecting possible physical interventions with your laptop is extremely difficult. If you do need to securely store your laptop for some reason (for example, if you wish to cross a country's border without your laptop) you should try to do so in a way whereby any security breach would be detectable. Be creative - but it will be a challenge to outsmart a sophisticated adversary. Ideally, you will leave it under the close protection of someone you trust, if you cannot guard it yourself.

Snowden developed the app 'Haven' in 2017 that you can use for OpSec. Be creative, but it will prove to be a challenge to be smarter than a capable adversary. Sometimes it is even clear you laptop has been compromised (by missing or damaged screws for example).

For technological defence against low levels of risk, and as a general safety measure, you could download an open source application called Prey: see https://preyproject.com. This is tracking software that helps users find, lock and recover their computers. It also enables you to take screenshots of the stolen laptop's screen, and to activate the webcam to take a photo of its new owner. Downloading tracking software may feel counter-intuitive for a journalist who wants to strictly defend their privacy! Since the application is open source, it is thought to be fairly trustworthy. However, a sophisticated adversary will not be caught out by it. It is only recommended that you use this application as a defence against less advanced adversaries.

If you wish to continue using non-securable hardware, there are still measures you can take to protect you data and communications from less intrusive surveillance activities – so do read on. Just be aware that, if you become a surveillance target of someone with the resources, ability, and motivation to obtain your data, it is a fait accompli.

2.

Operating System

If your hardware is secure against automated and pre-positioned surveillance, it is vital to prevent the introduction of software that will make the system vulnerable again. Even if you are operating at low-risk levels, using the right software can help protect the security of your data and communications from automated and dragnet surveillance.

The most important software on a computer, in addition to the firmware (see 'Firmware' in Chapter 1), is the operating system. This is the software that takes control of the computer as it boots up and is the interface through which you use the computer. In short, the operating system tells the computer what to do, and how to do it. Popular operating systems include versions of Windows (e.g. XP, Vista, 8, 10), OS X (for Mac), and Linux distributions.

We now know that intelligence agencies often have access to 'backdoors' in popular operating systems, which enable them to gain covert access to users' data.

Threats associated with operating systems:

- Malware, viruses
- Surveillance 'backdoors' within an operating system, accessible to the intelligence community

Two key measures are important for protection against operating system threats:

- Use an open source operating system (for medium risk)
- Use Tails, an amnesic, incognito operating system (for high - top risk)

2.1 Open source operating systems

To increase confidence that your operating system does not have potential surveillance 'backdoors' (i.e. that it cannot be abused for surveillance purposes), it should be 'open source'. 'Open source' software is freely distributed software for which the source-code, the very fabric of the operating system, is 'open' and publicly available. This allows independent experts to view the source code anytime, and verify that there are no security flaws in the makeup of the operating system. A full, ten-point definition is available at www.opensource.org/osd.

Furthermore, open source operating systems are less susceptible to malware (malicious software, typically spyware) and viruses. This is because they are much less frequently used than proprietary operating systems and have a correspondingly low market share.

Open source software

Open source software is also known as ‘free software’ – not only for the freedom of access to its source code, but because it is also distributed on a free/donations-only basis.

It should be noted that open source software is only as trustworthy as the trust one puts in the expertise and frequency with which the source code is created and examined. However, open source software that is widely used is more likely to be frequently examined, and is preferable (at least for InfoSec purposes) to closed source software.

Operating systems by Microsoft and Apple (e.g. Windows, OS X) are closed source, and are expected to contain surveillance backdoors accessible to GCHQ, the NSA and allied interests. Microsoft’s operating systems are particularly unsuitable, since more of its code is closed source than Apple’s code, and their systems are more susceptible to malware and viruses. Such closed source operating systems are unsuitable for important data and communications if you think you, or someone you are communicating with, could be (or become) a target of surveillance.

Note: closed source mobile operating systems, such as iOS and Android, are ubiquitous on smart phones, which are therefore indefensible against targeted attacks – see chapter 7 for mobile InfoSec.

2.2 Linux

Linux is the leading open source, community developed, operating system. There are many different versions of Linux operating systems that you can use.

2.3 Ubuntu

ubuntu.com

Ubuntu is the most widely used Linux operating system. It is easy to install, highly functional, and user friendly.

You can replace your Windows operating system with Ubuntu, or you can run both Windows and Ubuntu on the same laptop (should you wish to familiarise with the new system before committing to it). Ubuntu is very user friendly and not too dissimilar from other operating systems, so we would recommend the former - that you replace your Windows operating system with Ubuntu. This removes the Windows operating system altogether, which is recommended for InfoSec purposes (otherwise, potential ‘backdoors’ may remain). Note that removing your old operating system will also remove all files associated with it – so be sure to backup any files you wish to keep that are on that laptop.

It is not recommended that inexperienced users wipe a MacBook of its operating system in order to install Ubuntu, as this could cause problems with a Mac’s functionality. You could use Ubuntu through a ‘virtual machine' on a Mac, but we will not discuss that here – it is unclear what security advantages can be achieved by simultaneously running the two operating systems.

It should be noted that a few elements within Ubuntu are currently closed source – it is assumed (though not definitively known) that these do not pose a security risk. However, other popular variations of Linux, including Debian and Trisquel, are entirely open source. Note that they may be slightly less intuitive for those new to Linux to use and maintain.

2.4 Tails

tails.boum.org

Use an amnesic, incognito operating system for the greatest security: Tails. Tails stands for 'The Amnesic Incognito Live System'. It is an open source, Linux-based operating system that protects users' privacy and anonymity.

- **Amnesic:** because no trace of your computer use is left on the system after shut down
- **Incognito:** because it is privacy and security orientated, accessing internet anonymously by default, and thus circumventing any censorship

Tails is purposefully designed as an anti-surveillance system, and comes with several built-in (entirely open source) security-oriented applications:

Built-in online anonymity

Once connected to the internet, various software on our computers frequently send and receive packets of data via the internet, whether in active use or not. We know that intelligence agencies routinely surveil this network activity and are working to increase this surveillance. However, all software on Tails is configured to connect to the internet anonymously, via Tor (see chapter 3), thus protecting you from network surveillance.

Furthermore, the in-built Tor web browser includes popular security extensions like HTTPS Encryption and HTTPS Everywhere which encrypt your browsing data; Adblock Plus to block ads and tracking; and NoScript to block harmful JavaScript and Flash (as they can compromise anonymity). Using Tails on its high security settings can mean some web features won't work – but it is a worthwhile compromise for an incomparable privacy gain when working on sensitive projects. Alternatively, you can lower the security settings (in Tor's security slider) or use the 'Unsafe Browser' on Tails.

Note: if you use the unsafe browser, or attempt to log in to an online account that is clearly linked to your real identity on any browser, you will compromise your anonymity for that entire Tails session. Shutdown and restart Tails every time you use a new identity. Files and documents can also contain metadata that may indicate your location via GPS – see chapter 4 for tips on removing such metadata.

Built-in encrypted email and chat

Tails offers in-built encrypted and private messaging. Tails includes the Icedove (Thunderbird) email client with OpenPGP for email encryption (see chapter 5) and the instant messaging client Pidgin (see chapter 6) which supports private and anonymous messaging.

Built-in file encryption

Tails comes with LUKS, to encrypt files. If you want to store files on the same USB stick you are running Tails from, you can create permanent storage space, or a 'persistent volume' on the USB stick. Tails will encrypt the persistent volume by default, requesting your password to view or access any of the files stored.

Expert info: Whilst the persistent volume is useful for storing relatively unimportant information and documents, you should not use it to store or transport the most sensitive documents. This is because the persistent volume is not 'hidden'. That is, should an adversary obtain the USB stick, they will be able to see that an encrypted volume exists on the device, and they may force or trick you into giving them the password. You should create a 'hidden' volume for the most sensitive documents (perhaps on a different USB stick), which appears to take up no memory – only you know it is there. This can be easily done with an application called VeraCrypt – see chapter 4.

2.4.1 Built in password protection

Tails comes preloaded with KeePassX, a password manager that stores usernames and passwords in an encrypted, local database, protected by your master password. It also comes with PWGen, a strong random password generator.

Tails is designed for use from a USB stick independently of the computer's original operating system. This means that you can remove your laptop's hard disk drive (recommended for high-risk work), but still boot up the laptop through a Tails USB stick. Alternatively, you can put a Tails USB stick into a computer with the hard disk drive intact, and boot up via Tails – the machine will ignore the original hard disk and operating system, and run from the USB drive with Tails instead.

The provision of a 'mini system' on a Tails USB stick makes it ideal for sensitive journalistic projects. Your machine can essentially be 'clean' with no trace of your work on there, and your documents can be stored on the highly portable, inexpensive USB stick. Tails even comes preloaded with open source editing software such as LibreOffice for creating, reading and editing documents, PiTiVifor editing videos, and Audacity for editing sound.

The USB stick is ideal for travelling, and you can plug it into any computer, if you set the computer to boot up from USB (explained within instructions below). It is wise to have separate Tails USB sticks for separate projects, to spread your identity trace and minimise the risk, should you lose a USB stick. If appropriate, you could also give a prepared Tails USB stick to your source, with a few instructions, so they have secure means of communicating with you. In high risk scenarios, you may wish to use Tails on an entirely separate machine to your usual laptop (see Chapter 1, ‘Top risk level’).

Using Ubuntu is a good option for day-to-day, non-sensitive work. However, it is wise to also create a Tails USB stick and switch over to Tails when working on sensitive projects – particularly when working with important documents, communicating with high-risk individuals, or researching for sensitive projects online. Furthermore, taking serious InfoSec measures pre-emptively can prolong your anonymity and thus the time you, and most importantly your source, have before you become targeted for surveillance.

You have now learnt how to robustly protect your system. In the following chapters, you will learn how to protect your communications, anonymise your browsing data, and encrypt and transport sensitive documents.

2.5 Step-by-step instructions

2.5.1 Installing Ubuntu

Note: all Windows documents, programs, files, etc. will be deleted if you replace Windows with Ubuntu (recommended).

1. Download Ubuntu

Download Ubuntu from http://www.ubuntu.com/download/desktop. You will need to know how much RAM your laptop has, and download either 32-bit (for older machines, such as the recommended ThinkPads, with 2GB or less RAM) or 64-bit (for newer machines with 4GB or more RAM). The download may take 20-60 minutes.

2. Download Linux's USB Installer

Go to http://www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows, click 'Download Pen Drive Linux's USB Installer ›', and scroll down to click on the big 'Download UUI' button. This will download the USB installer, allowing you to store Ubuntu on a USB drive, which you will use to install Ubuntu.

Expert info: During the installation, the hard disk cannot run any other software – so you need another source, in this case a USB stick, to run the install software.

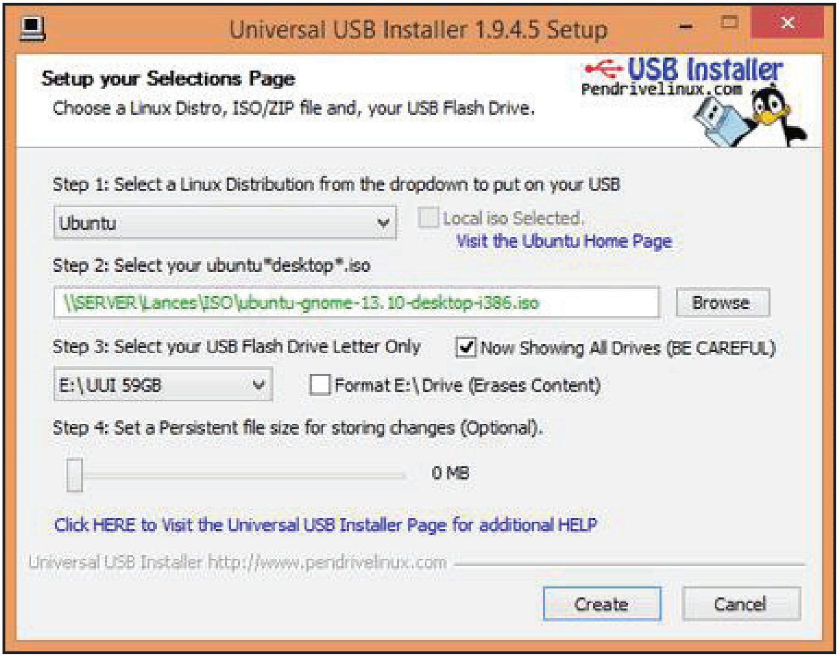
3. Put Ubuntu on the USB Installer

When both downloads are complete, insert a clean USB stick and open the USB Installer.

Select the Linux Distribution from the dropdown menu (Ubuntu); use the 'Browse' button to locate the Ubuntu download; and select the USB

Flash Drive Letter (where the computer has located your USB stick). Click ‘Create’.

When this is complete, safely remove the USB stick, and shut down the computer.



Universal USB Installer 1.9.4.5 Setup

Setup your Selections Page

Choose a Linux Distro, ISO/ZIP file and, your USB Flash Drive.

Step 1: Select a Linux Distribution from the dropdown to put on your USB

Ubuntu

□ Local iso Selected.

Visit the Ubuntu Home Page

Step 2: Select your ubuntu*desktop*.iso

\\SERVER\Lances\ISO\ubuntu-gnome-13.10-desktop-i386.iso

Step 3: Select your USB Flash Drive Letter Only

☑ Now Showing All Drives (BE CAREFUL)

E:\UUI 59GB

□ Format E:\ Drive (Erases Content)

Step 4: Set a Persistent file size for storing changes (Optional).

0 MB

Click HERE to Visit the Universal USB Installer Page for additional HELP

Universal USB Installer http://www.pendrivelinux.com

Install Ubuntu Booting from USB

You need to set your machine to boot from USB – a setting that is located in the BIOS menu of your laptop. You can access the BIOS menu as your machine powers up. Before attempting this, you may wish to search online to find out which key to press to access the BIOS menu on your particular laptop. On many machines an 'entering setup' message appears as it powers up, informing you that you can press [key] to enter BIOS/setup/system configuration, in which case you can follow that instruction. It is often a key such as F1, F2, F3, F12 or DEL.

You may also wish to research how, via your particular machine's BIOS menu, to boot the machine from the USB drive. Insert the USB stick into the laptop whilst switched off, then boot up and enter the BIOS menu. This setting may be in a menu item such as Startup > Boot; or a menu tab such as 'Boot', 'Boot options', or 'Boot selection menu'. Select your USB drive, or make sure your USB drive is top of any boot priority order (if an item on the list has a '+' it means it has a submenu, where your USB listing may be hiding!). You can often change the order using + and – keys. Navigate to the 'Exit' or 'Save and exit' menu, and select 'Exit saving changes' (or similar) option to make sure your boot preference has been saved.

So: power up the laptop with the USB stick already inserted, enter the BIOS menu, and opt to boot from your USB drive.

After saving and exiting the BIOS menu, the machine should boot from the USB and thus the Ubuntu installer boot menu should load.

Select 'Install Ubuntu on a Hard Disk'. The automatic installer will now guide you through the Ubuntu set up.

You may be prompted to set up Wi-Fi, but you don't have to worry about setting up Wi-Fi now, especially if you have removed your Wi-Fi card.

Under 'Installation type':

- Select: Replace Windows with Ubuntu (if you want to wipe Windows)
- Select: Encrypt the new Ubuntu installation for security
- Select: Use LVM with the new Ubuntu installation Choose a strong password (see chapter 8 for guidance).

The software will ask you to register your name (but you don't have to enter anything here). Pick a computer name and username for your log-in. Choose a strong password, and tick 'require my password to log in' and 'encrypt my home folder'.

Ubuntu will now complete the install. Once installed, turn off the laptop and remove the USB. Turn the laptop on and Ubuntu should launch!

When you connect to the internet, go to the top left Ubuntu icon on the desktop and search 'updates'. Click to accept any updates.

Ubuntu privacy tweaks

1. Select 'System Settings' on the desktop > Security and Privacy
2. Under 'Files and Applications' you can control whether records are kept of your file and applications usage.
3. Under 'Search' you can disable online search results when searching in the Dash. This stops Ubuntu's Amazon integration, and prevents your Dash searches being sent back to Ubuntu servers and Amazon. You can right-click the Amazon icon on the desktop and select 'Unlock from Launcher' to remove it from the desktop.

4. Under 'Diagnostics' you can opt out of sending 'error reports' and 'occasional system information' to Canonical.

2.5.2 Installing Tails

There are several ways to create a Tails USB stick:

1. Via a cloned Tails USB stick from a trusted source (recommended - contact infosec@tcij.org for help finding a cloned Tails stick)
2. Manually via TailsInstaller (requires Ubuntu 15.10 or later)
3. Manually via GNOME Disks (Ubuntu)
4. Manually via Universal USB Installer (Windows)
5. Manually via the command line (Mac. N.B. this is the most difficult method)

We highly recommend starting with Tails via a cloned USB stick. Manual installation is not always easy, and as such does not have a perfect success rate.

Installation tips:

- Before you start the installation, prepare your USB stick/s. Tails include instructions for doing so in Windows and Mac installation guides – to prepare sticks on Ubuntu, see the next page.
- Before attempting your first boot-up using a Tails USB stick (including any intermediary Tails stick if installing manually) you should set your machine to boot from USB. See 'Install Ubuntu Booting from USB' on page 349'.

- We recommend downloading Tails via the Firefox browser. This is because there is a 'Tails Download and Verify' extension available for Firefox, which automatically verifies that your download is the intended download and has not been tampered with. (The link and instructions for this extension are within Tails' installation instructions)
- Instructions for the variety of installation methods can be found on the Tails website, here: https://tails.boum.org/install/index.en.html.

Note: whilst many more users are successfully using the latest versions of Tails from Mac computers, Tails developers have less experience using Mac and problems (such as inability to access WiFi) have been reported.

Clean and prepare the USB stick (Ubuntu)

You will need a USB stick which is 4GB or bigger – ideally 16GB if you intend on storing documents on it too. Perhaps you have used this USB stick before, or perhaps it came with pre-installed software. Either way, opening the USB drive on a computer and moving the files to Trash only stops them being visibly listed, and does not really 'delete' them. For your new Tails USB stick, you want to start with a totally clean device.

We also need to change some settings on the USB stick, so that it is prepared to boot up the computer and host Tails.

1. Install GParted - Go to the Ubuntu Software Centre on your computer, and search for 'GParted'. Install.
2. Insert your USB stick into the laptop.

3. Open GParted. Go to GParted > Refresh Devices
4. Your USB should appear as a drive in the top right drop down menu (e.g. listed as /dev/sdb or dev/sdc) and will display the size of the available space on the USB stick. Select this device.
5. Now at the top of the window is a long rectangle, outlined green, possibly with some space on the left of the rectangle shaded yellow. Right click, select 'unmount'; right click again, and select 'delete'.
6. Any colours in the rectangle are now gone and replaced by grey. Right click on the rectangle, and select 'New'.
7. A screen titled 'Create new Partition' appears. Under 'File System' select 'fat32', and under 'Label' type 'TAILS'. Click 'Add'. fat32 = File Allocation Table 32 bits
8. Click the green 'tick' (just under the 'Partition' option on the toolbar at the top of the window)
9. In the pop up box, select 'Apply' to apply operations to device, and 'Close' when the message appears: "All operations successfully completed".
10. Now, right click on the long green rectangle and click 'Manage Flags' > select 'boot', and close.

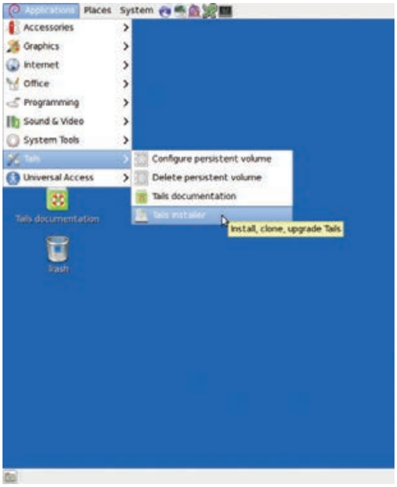
This will tell the computer that this is a drive that can be used to start the system from. You can safely remove the USB stick – it is ready for a Tails installation.

Cloning Tails USB sticks

If you receive a cloned Tails USB stick, all you have to do is set your machine to boot from the USB drive (see 'Install Ubuntu Booting from USB' on page 349), and insert your Tails stick to get started.

If you wish to clone a Tails USB stick (for example, if you are making your own Tails stick by cloning a friend's, or if you are cloning your own Tails stick to equip a source or colleagues), follow these instructions.

Prepare a new clean, bootable USB stick (4 GB or more) with GParted, as before (see 'Clean and prepare the USB stick (Ubuntu)' on page 353), to clone Tails to.



1. Start the Tails system with your current Tails stick
2. Insert the clean, bootable USB-drive into one of the free USB-ports on the computer.
3. On the Tails desktop go to Applications > Tails > Tails Installer.
4. A new window will open. Select: Install by cloning
5. The Tails Installer window should list your clean USB stick under 'Target Device'. Click 'Install Tails' on the bottom of the window and click 'Yes' on the pop-up window to confirm your device selection. A

clone of your Tails installation will now be made to the other USB drive.

When done the Tails Installer will tell you: Installation complete! When completed, shutdown the system and try to start from the newly created drive to ensure it works properly.

Upgrading Tails

Your Tails system should automatically look for, and download, updates. It is important to keep your system updated. After booting Tails and connecting to Tor, if an upgrade is available, a dialog box appears and proposes you to upgrade the system.

However, it can often take a while for Tails to connect to the internet after booting, in which case it may be unable to check for upgrades at start up. You can check for upgrades anytime by opening the Terminal (black box icon on the top toolbar on the Tails desktop) and typing the following command: tails-upgrade-frontend-wrapper

And press enter. Tails will check for updates, or inform you whether your system is up to date.

More information on upgrading Tails, and troubleshooting when Tails does not upgrade automatically, can be found on the Tails website:
https://tails.boum.org/doc/first_steps/upgrade/index.en.html

Using Tails

First, you need to instruct your laptop to boot up from a USB drive – see 'Install Ubuntu Booting from USB' on page 349 for instructions.

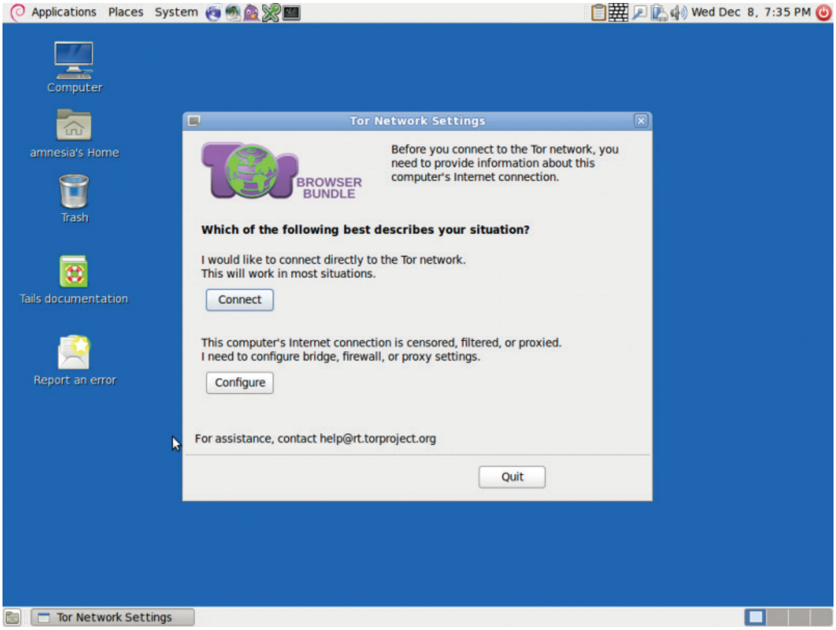
When you boot up in Tails, you will see a screen load up with options 'Live' and 'Live failsafe'. Use the arrow keys to highlight 'Live' and hit the enter key.

You will then be offered, 'More options?'. It is not essential that you enter this menu, unless you need to configure Tails to circumvent Tor censorship. Otherwise you can select no, 'Login', and start exploring Tails. If you do select yes for more options, you will see:

- **'Administrative password'**. It is unlikely you would need to create one unless you want to access the internal hard disk of the computer (which is not recommended, and can lead to unnecessary security risks).
- **'Spoof all MAC addresses'**, which should be automatically selected. This is a good option to hide the serial numbers of your network cards, and thus is another function that helps to hide your location.
- **'Network configuration'**, under which you have two options: connect directly to the Tor network, or 'This computer's internet connection is censored, filtered or proxied. You need to configure bridge, firewall or proxy settings'. If your network does not allow Tor connections, select the latter.
- **'Disable all networking'** if you wish to have offline use

Using Tails via bridges/circumventing censorship

This helps people to connect to the Tor network in situations where their network disallows Tor connections. Bridges are Tor relays (nodes or computer points that receive traffic on the Tor network and pass it along) that help circumvent censorship.



Tor Network Settings

Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

Which of the following best describes your situation?

I would like to connect directly to the Tor network.
This will work in most situations.

Connect

This computer's Internet connection is censored, filtered, or proxied.
I need to configure bridge, firewall, or proxy settings.

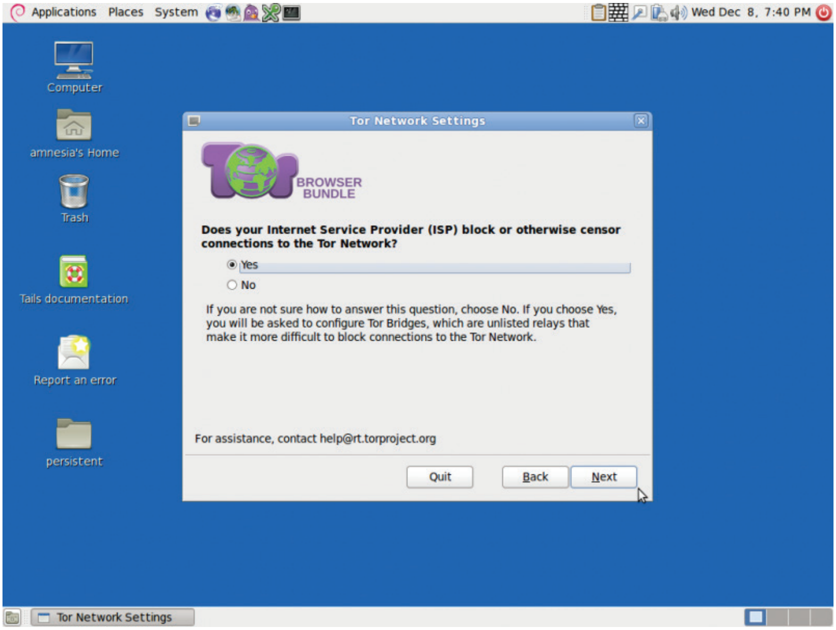
Configure

For assistance, contact help@rt.torproject.org

Quit

When you boot up using the Tails USB stick and are offered 'More options?', select 'Yes' and continue. Under 'Network configuration', select 'This computer's internet connection is censored, filtered of proxied. You need to configure bridge, firewall or proxy settings'.

Then, when you connect to the internet the Tor browser bundle window will appear asking the same question.



Does your Internet Service Provider (ISP) block or otherwise censor connections to the Tor Network?

● Yes

○ No

If you are not sure how to answer this question, choose No. If you choose Yes, you will be asked to configure Tor Bridges, which are unlisted relays that make it more difficult to block connections to the Tor Network.

For assistance, contact help@rt.torproject.org

You now have a box to enter one or more ‘bridges’ - strings of numbers that identify a Tor relay. To get bridges, go to https://bridges.torproject.org or if you cannot access that site, send an email to bridges@torproject.org from a gmail.com or yahoo.com email address, with the line ‘get bridges’ by itself in the body of the message, and some should be sent back to you. Using a bridge can be an extremely slow way of connecting to the internet – but if you need it to circumvent censorship, it works very well.

Persistent storage space on your Tails USB stick.

To create a persistent volume in Tails, go to Applications > Tails > Configure persistent volume. Once you have entered a (very strong, see chapter 8) password, you can choose what types of files you will save in the persistent volume. You could select all types, to keep your options open.

Now, every time you boot up with the Tails USB stick, you will be asked two questions: 'Use persistence?' and 'More options?' (as before). If you click 'Yes' to 'use persistence' and enter the password, you can access any data (e.g. configured email client, IM client, password manager, or files) you have saved to the persistent volume in previous sessions.

Using KeePassX

KeePassX is a password manager that stores usernames and passwords in a local encrypted database, protected by a master password. It also comes with PWGen, a strong random password generator. You will find KeePassX in Applications > Accessories > KeePassX.

- **To create a new password database:**

  File > New database. Create a strong master password that will protect your password database. You can then name your database file and choose the location where it will be saved.

  Groups > New groups (e.g. 'Jabber' group, for your Jabber usernames and passwords – more on Jabber in chapter 6).

- **To add a new password:**

  Click on a group > Entries > Add new entry. Here you have the option of entering a password, or generating a random one (click 'Gen'). If you click on the eye icon, you can see the text of the password – otherwise, it will remain obscured.

- **To retrieve a password**:

  When you have added a password to a group, you can right click on the desired password and select 'copy password to clipboard'. You can then paste it in to a login form.

Email in Tails

NOTE: You should read chapter 5 on email before continuing to read the rest of this chapter. Also see Tails' documentation on Icedove (Thunderbird) at: https://tails.boum.org/doc/anonymous_internet/icedove/index.en.html.

Tails comes with a pre-installed mail client, Icedove (this is a rebranded copy of Thunderbird, which is documented in chapter 5). It is also pre-installed with Enigmail, an extension for Icedove which supports email encryption. If you are used to using Thunderbird/Enigmail and encrypting email on your regular operating system, you should have no problem using Icedove on Tails, and the instructions in chapter 5 also apply here.

- **Importing your key from another laptop/operating system**

  Lots of people use separate Tails sticks, email addresses, PGP keys, etc., for different projects, which is a great way to work securely and compartmentalise your activities. However, you may wish to add a key that was made on another laptop to your Tails key manager (but consider whether this could compromise your anonymity on Tails). For this, you'll need a spare USB stick.

Insert a USB stick into the laptop that has the key you wish to move. Open Thunderbird, and go to Enigmail > Key management. Find your email address/key on your contact list and right-click it to select > Export keys to file > Export secret keys. Find your USB device and select it as the location to save your key to. Safely remove the USB device.

Start up your Tails system. Once Tails has booted up and connected to the internet, insert the USB device with your key saved on it. Click on Tails' OpenPGP encryption applet (the clipboard icon on the top right of the menu bar) and select > Manage keys > File > Import. Open your USB device files to find the key to import, and select Import.

Once you have imported your key to Tails, you may wish to securely delete your key from the USB device you used to transport it, as it is unwise to have your secret key saved on an unprotected USB device/s. Using the 'Wipe' function on Tails (right-click on the key file on the USB device) will securely delete the file.

- **OpenPGP encryption applet**

Because *all* internet connections on Tails run through the Tor network, connections to your email provider via your email client will also be run through Tor. Users of some email providers sometimes have problems configuring their email accounts with Icedove through Tails, because the connection is re-routed through the Tor network to disguise your location.

Tails offers an alternative method you can use to encrypt email and email attachments. Rather than using an email client to encrypt the entire email, you can highlight text and encrypt it to the desired recipient's key, before pasting the encrypted text into an email (e.g. when composing email on the web browser).

- **Import contact's public ke**y

Go to the OpenPGP encryption applet (the clipboard icon in the top right of the top menu toolbar) > Manage keys > then either:

  - Remote > Find remote keys (if you do not already have the person's key). Enter the contact's name, and click search.

Or:

  - File > Import (if you have the key already saved in a file).

- **Encrypt the text**

Applications (left on the top menu toolbar) > Accessories > gedit Text Editor. Type your message. Then select all (Ctrl + A) and copy (Ctrl + C, or right click > copy) the message to the clipboard. Go to the OpenPGP encryption applet > Sign/encrypt Clipboard with Public Keys > select the recipient of your email (you need to have already imported their key), sign the message as the email address from which you will be sending the email, and click OK. Then paste the message (Ctrl + V) into the composing window in your email account, and send.

Note that you have encrypted the message to only allow decryption by the desired recipient. This means that once encrypted, you cannot decrypt it to read it yourself. Therefore, if you use this method, it is a good idea to select your own public key, as well as that of the recipient of the email, when you encrypt the message. You will then be able to decrypt it if you want to read your sent messages.

- **Decrypt the text**

Select the encrypted text that you want to decrypt. Include the lines "-----BEGIN PGP MESSAGE-----" and "-----END PGP MESSAGE-----". Copy the text to the clipboard (Ctrl + C, or right click > copy). The OpenPGP Applet (clipboard icon) now shows a padlock, meaning that it contains encrypted text. If the text that you selected is only signed but not encrypted, the OpenPGP Applet now shows a seal, meaning that the clipboard contains signed text.

Click on the OpenPGP Applet (clipboard icon) and select 'Decrypt/ Verify Clipboard' from the menu. The decrypted text appears in the Output of GnuPG text box.

- **Encrypting email attachments**

It is easy to encrypt files using public keys and to send these as email attachments with Tails. Right click the desired file > Encrypt > tick the recipient’s email address (sign the message as the address from which you will send the email) > OK. You will now see a duplicate of the selected file, with the ‘.pgp’ extension – this means it is an encrypted file. Attach the .pgp file to your email, which can only be decrypted and opened by your chosen recipient.

3.

Safe Browsing

Web browsing risks:

- Data collection of your identity
- Data collection of your browsing behaviours, including the pages you have visited, and when
- Data collection of your passwords and autofill information
- Data collection of your location (and previous locations)
- Malware (malicious software, sometimes spyware) injections
- Being blocked from accessing certain sites
- Being blocked from using anonymous browsers

InfoSec action:

- Use a general purpose browser, with privacy-enhancing extensions, for daily activities
- Use the Tor browser for anonymous browsing, for censorship resistance, and to hide your real location

A web browser is the software you use to access the World Wide Web. For many of us, web browsing is ‘The Internet’, and in many senses it is a window to the world.

Because of the huge opportunities in web browsing, some states impose restrictions on access to certain websites, which impedes people’s freedom, and of course poses a problem to local journalists, researchers, and foreign correspondents. Whilst web access is largely unrestricted in the West, we have serious privacy issues with our web browsing. It remains that most service providers and websites collect vast amounts of data about their users. The British Government is currently trying to pass legislation that would force internet providers to record every single internet connection of every single person, including location data and device identifiers.

This chapter explains some options to minimise the impositions on freedom and privacy in web browsing, under a range of circumstances.

3.1 What browsers to use

Many people are unaware of the privacy issues with browsers, and use whatever browser is already on their system. However, there are alternatives that are more integrally secure, and that can be vastly improved by adding 'extensions' – extra software that improves the functionality of your browser.

While there are dozens of browsers with specialised purposes, here we will recommend three open source browsers:

- Brave Browser[8] or Midori Web Browser[9] and Chromium[10] or perhaps Firefox as a general purpose web browser for Linux and Windows
- Chromium, as a general purpose web browser for Mac
- Tor[11] as a secure browser that anonymises your location and identity, and overcomes web censorship (suitable for Linux, Windows and Mac).

We recommend Firefox for Linux and Windows but not Mac as Firefox can conflict with Tor on a Mac (Firefox and Tor are based on the same code).

3.1.1 A general-purpose browser

Your daily web browsing centres around generally unrestricted sites and sites that you log in to, such as social media platforms, LinkedIn, newspapers, YouTube, shops, and so on.

Firefox

A popular open source web-browser.

[8] *https://brave.com/*

[9] *https://www.midori-browser.org/*

[10] *https://www.chromium.org/Home*

[11] *https://www.torproject.org/*

For Windows, download Firefox for your operating system and language at www.getfirefox.com. On Linux distributions/Ubuntu, Firefox should already be installed.

Brave and Midori

Less known, but safe open source browser are Brave Browser[12] of Midori Web Browser.[13]

Chromium

An open source clone of Google Chrome, without the additional Google services. Download Chromium for Mac at https://www.macupdate.com/app/mac/36244/chromium.

Alternatively, go to https://www.macupdate.com and search for Chromium.

Extensions to enhance privacy

A general-purpose browser is certain to make your identity, location and activity available. However, there are some extensions we can use to increase our privacy and security somewhat. You can find a range of privacy enhancing extensions at https://addons.mozilla.org/en-US/firefox/

[12] *https://brave.com/*

[13] *https://www.midori-browser.org/*

extensions/privacy-security/, which should be suitable for both Firefox and Chromium.

We particularly recommend the following open source extensions:

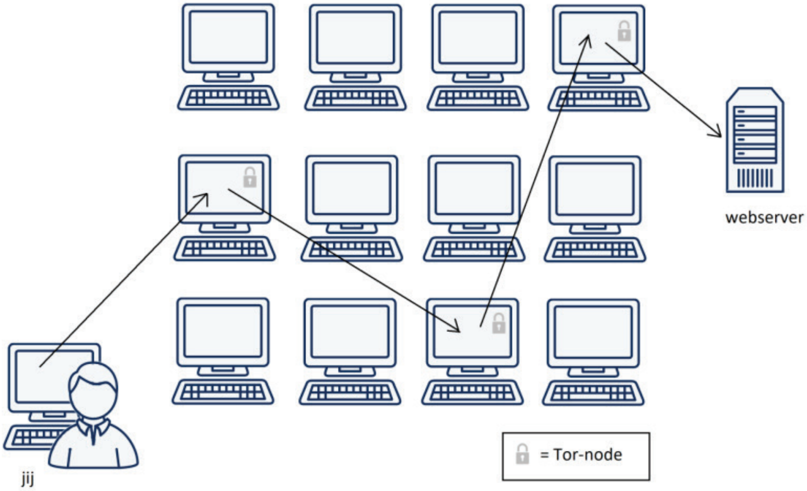
- **HTTPS Everywhere:** forces encryption for all connections between your web browser and the webserver you are visiting. https://www.eff.org/https-everywhere
- **NoScript:** blocks JavaScript. JavaScript is an essential element of many websites, but can be exploited to track your browsing behaviour, leak your passwords, and to inject malware. NoScript is very effective but you will need to grant or deny privileges on a per website basis depending on how much you trust them. https://noscript.net/
- **Ghostery:** blocks a wide range of trackers in its database, which track your browsing behaviour. Do make sure to switch off 'GhostRank' under Settings > Options, as this itself reports back data for marketing purposes. https://ghostery.com
- **LastPass:** is a password generator and manager for Firefox. https://lastpass.com/

3.1.2 Browser for anonymous surfing: Tor

https://www.torproject.org/

About Tor

The Tor browser was especially designed for anonymity by routing all its traffic through the Tor ('The Onion Router') network. Therefore, this browser prevents internet providers storing accurate information about your web browsing history.



How Tor works

The Tor network is a global network of computers called Tor nodes that have encrypted connections with each other. When the Tor browser starts, it will connect to one of these nodes. This node will connect to a second node that will in turn connect to a third node. These nodes could be anywhere in the world, and the first and third node will not be aware of each other. The third node will connect to the wider internet and fetch webpages from the sites you're visiting. Those sites will not be able to see where you are or who you are (as long as you do not identify yourself by logging into services associated with your real identity).

Since the Tor browser runs all its traffic trough several other places around the world it is slower than regular browsing but this is a price well worth paying for being online anonymously.

In order to ensure the safety of the browser, Tor automatically enables HTTPS-Everywhere, and automatically avoids extensions such as Flash, RealPlayer, and QuickTime. However, you can adjust the settings to improve usability as you like.

Overcoming restrictions and blocks to Tor

If the network provider you are using (this may be the entire country or just a University network) blocks access to the Tor network, you can use 'bridges' to achieve access.

Bridges are 'private' Tor relays (nodes or computer points that receive traffic on the Tor network and pass it along) that are less likely to be blocked, and thus help circumvent censorship.

This is how you use bridges: launch the Tor Browser. Click on the green onion (to the left of the address bar) and click Tor Network Settings > tick 'My ISP blocks connections to the Tor network'.

You now have a box to enter one or more 'bridges' - strings of numbers that identify a Tor relay. To get bridges, go to https://bridges.torproject.org or if you cannot access that site, send an email to bridges@torproject.org , from a gmail.com or yahoo.com email address, with the line 'get bridges' by itself in the body of the message, and bridges should be sent back to you. Using a bridge can be an extremely slow way of connecting to the internet – but if you need it to circumvent censorship, it works very well.

Staying anonymous

The latest version of the Tor browser gives users a security slider to determine their security options. In the Tor browser, click on the green onion (to the left of the address bar) and select 'Privacy and Security Settings' to see the slider and the various options. The slider is set to *low* by default, which increases usability. To benefit from the high level of privacy that Tor can offer, or if you need to browse anonymously, you should set the slider to the highest level.

Do not open documents (such as .doc and .pdf) downloaded via Tor while still being online. These document formats can contain elements that independently connect to the internet, thereby revealing your real IP address. Make sure you are offline first or use a separate computer for working with such documents.

Don't run bittorrent over Tor since this may betray your real IP address and will consume disproportionate amounts of capacity on the Tor network.

Make sure you use the latest version of the Tor browser. You will be alerted on the Tor browser homepage when updates are available, or you can click on the green onion in the browser window (to the left of the address bar) to 'Check for Tor Browser update'.

Install Tor

- **Mac, Windows:**

  Download and install the Tor browser for your operating system at https://www.torproject.org/ following the installation instructions on the site.

- **Linux/Ubuntu:**

  1. Download the Tor browser for Linux at https://www.torproject.org/, and select 'Save file'. Wait for the download to complete.
  2. In your file directory, go to Downloads (or wherever you saved the download), right click on the Tor download, andselect 'Extract here'. Open the extracted file (e.g. tor-browser_en-US), and

click ‘Tor browser setup’.

3. You now have the option whether to ‘Connect’ or ‘Configure’. Unless your network provider blocks access to the Tor network (in which case, refer to our previous section ‘Overcoming restrictions’), select ‘Connect’.
4. The Tor browser should now launch. The ‘Tor browser setup’ icon in your file directory should now be ‘Tor browser’ – this is your Tor launch icon. You can drag this icon to the desktop or lock it to the launch bar to make your Tor launcher easily accessible.

4.
Data

When storing or transporting data, there are several risks that require attention: interception/theft, loss, corruption and incrimination. The difference between interception and theft is detectability by the original owner. Interception usually means a data copy has been covertly made while theft would suggest the storage device (laptop, USB-drive or hard-disk) containing the data, or the original data, has been taken. The latter case would be detectable, whereas the former might not be.

Risks:

- Loss
- Corruption
- Interception
- Theft
- ‘Deleted’ data recoverability
- De-anonymising/compromising metadata

InfoSec actions:

- Back up data
- Encrypt data
- Securely share files
- Securely delete data
- Delete metadata

If sensitive data falls into the hands of adversaries, there may be severe consequences for sources or the journalist. To protect digital files there are several options. Simply storing the material on a small device (USB drive, memory card or external hard disk) and hiding it may be effective in certain cases. In such a scenario, the entire security of the material is dependent on the hidden device not being found. To protect your data from unauthorised access, it is also important to encrypt it. VeraCrypt is an easy-to-use tool for encrypting files and entire disks, and can even hide their very existence.

4.1 VeraCrypt for encyption

VeraCrypt is open source encryption software. VeraCrypt allows you to create an encrypted 'container' that acts as a digital strongbox for files, locked by a password. Once this box is created and filled with files it can be moved to an external storage device such as a USB drive, or sent over the internet to others. Even if the file is intercepted, the strongbox will not reveal its contents to anyone who does not have the password.

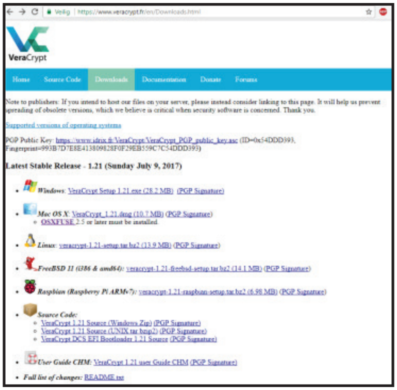
IMPORTANT! Do not forget your password, there is no other way to get to your data once it is encrypted. Losing you password means losing your data!

Download: https://www.veracrypt.fr/en/Downloads.html. Mac users will also need to download FUSE for OS X: https://osxfuse.github.io/) There is comprehensive documentation here: https://www.veracrypt.fr/en/Documentation.html

Installing VeraCrypt

On the VeraCrypt download page, select your operating system to be directed to the latest download suitable for your system.

Mac users will also need to download FUSE for OS X, which can be found here: https://osxfuse.github.io/



Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

Supported versions of operating systems

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x54DDD393, Fingerprint=993B7D7E8E413809828F0F29EB559C7C54DDD393)

Latest Stable Release - 1.21 (Sunday July 9, 2017)

- *Windows*: VeraCrypt Setup 1.21.exe (28.2 MB) (PGP Signature)
- *Mac OS X*: VeraCrypt_1.21.dmg (10.7 MB) (PGP Signature)
  - OSXFUSE 2.5 or later must be installed.
- *Linux*: veracrypt-1.21-setup.tar.bz2 (13.9 MB) (PGP Signature)
- *FreeBSD 11 (i386 & amd64)*: veracrypt-1.21-freebsd-setup.tar.bz2 (14.1 MB) (PGP Signature)
- *Raspbian (Raspberry Pi ARMv7)*: veracrypt-1.21-raspbian-setup.tar.bz2 (6.98 MB) (PGP Signature)
- *Source Code:*
  - VeraCrypt 1.21 Source (Windows Zip) (PGP Signature)
  - VeraCrypt 1.21 Source (UNIX tar.bzip2) (PGP Signature)
  - VeraCrypt DCS EFI Bootloader 1.21 Source (PGP Signature)
- *User Guide CHM:* VeraCrypt 1.21 user Guide CHM (PGP Signature)
- *Full list of changes:* README.txt

Encrypt a file with VeraCrypt

1. Download

Download VeraCrypt from https://www.veracrypt.fr/en/Downloads.html (and, if on Mac, FUSE for OS X: https://osxfuse.github.io/) and install on your system like any other application. VeraCrypt works the same on Windows, Mac and Linux systems and the encrypted containers are cross-compatible between these systems. This allows you to work securely with other people without having to know what system they use. An extensive guide: tutorial for VeraCrypt[14].

[14] *file:///C:/Program Files/VeraCrypt/docs/html/en/Beginner's Tutorial.html*

2. Create an encrypted volume

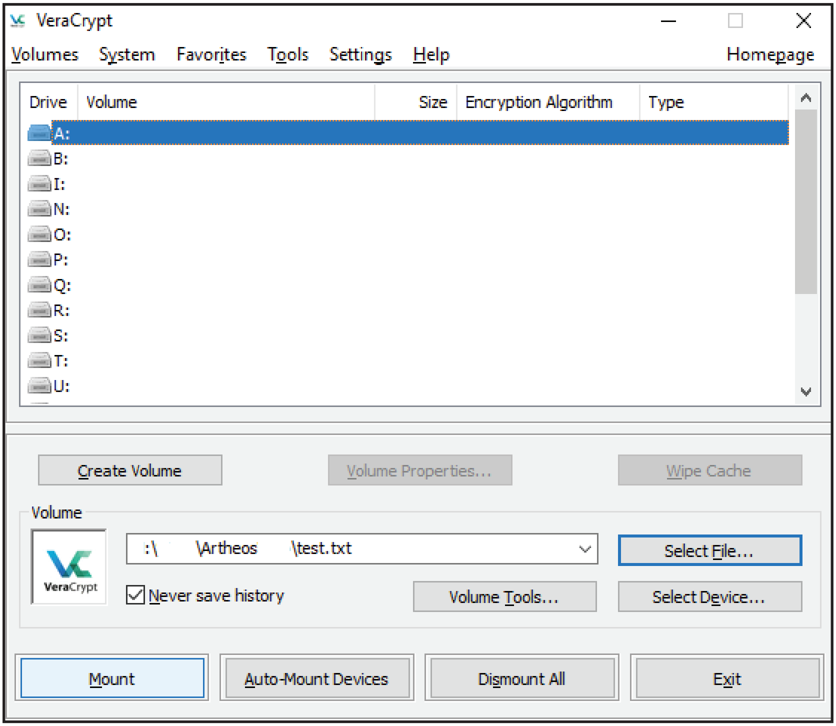
To create an encrypted 'volume' (like a folder) start the program and click:

1. 'Create Volume' > 'Create an encrypted file container' > select 'Standard VeraCrypt volume' > select the location where the container will be stored on your computer (it can be moved later) and give the container an (innocuous) name. *NOTE: To encrypt an entire external hard drive such as a USB stick, select 'Create Volume' > Create a volume within a partition/drive' Of course, you will need VeraCrypt to decrypt the USB drive, so if you are planning to decrypt on a computer on which VeraCrypt is not installed, you may wish to just create an encrypted container on the USB drive with your files, and also save VeraCrypt on the USB drive.*
2. The next screen is titled 'Encryption Options'. The default selections are fine. For the strongest encryption (encrypts multiple times), under 'Encryption Algorithm', select 'AES twoFish-Serpent', and under 'Hash Algorithm', select SHA-512.
3. The next screen is titled 'Volume size'. Select the size of the container (this will determine the maximum amount of data that can be put into it).
4. Set the volume password on the next screen. Make a good one (see chapter 8) and Do. Not. Forget!
5. The next screen is titled 'Format Options'. Select FAT. *EXPERT INFO: FAT is compatible with all systems but is limited in the maximum size of files it can contain (individual files cannot be larger than 4 GB). Usually this should not be a problem. If you need to be able to store larger files and are certain that choosing something other than FAT*

will not create problems with the sharing of the files, you could choose one of the other options.

6. The program will now generate a random dataset to encrypt the volume. Randomly move your mouse around for a moment, before clicking 'Format'. The program will now create the volume. Depending on the size, chosen encryption algorithm and speed of your computer this will take a few seconds to hours (for very large volumes).
7. Once the system is finished press 'Exit' to return to the main program screen.

Congratulations - you have created your secure volume!



Volume: :\ \Artheos \test.txt

☑ Never save history

Put the files you want to encrypt into your new encrypted volume. Now the volume can be ‘mounted’ (i.e. activated). Select any slot or drive. Click ‘Select File’ > locate and select the volume you just made > click ‘Mount’.

Now enter the password and click ‘OK’.

The VeraCrypt container will now appear on your system as a separate drive (much like a USB drive or external hard disk), and you can put files into it in the same way you would a USB drive (go to My Computer or Finder and click and drag files into the container).

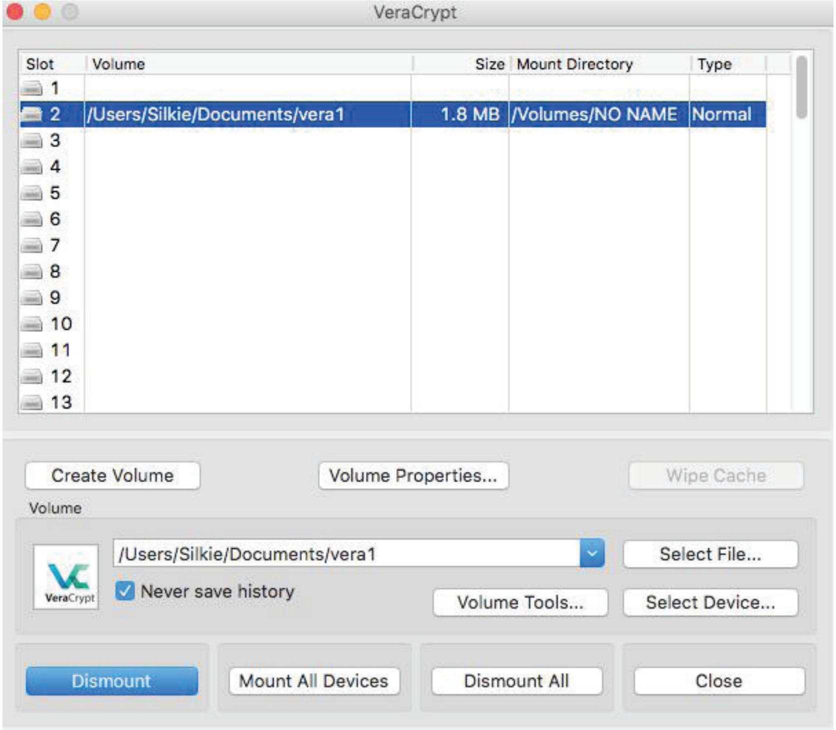
Once you have put the desired files in the container, ‘close’ the container by clicking ‘Dismount’ in VeraCrypt. The container will now appear to be just a file on your computer.

Hidden encrypted volumes

Hidden volumes are encrypted volumes that sit undetectably within a regular VeraCrypt volume. The purpose of this is to provide plausible deniability, and an extra layer of protection should your password be forced from you.

You will create a password for the regular VeraCrypt ‘outer’ volume – the container that is visible in your directory. Inside this container you will put sensitive files that you could plausibly want to encrypt and keep secret (unless this is a convincing decoy, an adversary could keep pressing for the ‘real’ password) – but that, if worst comes to worst, you are prepared to share with an adversary, should you be subjected to pressure.

However, within that volume is a hidden volume. No one can see it, and as far as we know, even the most sophisticated examination cannot reveal the existence of VeraCrypt's hidden volumes. Only the creator knows it is there. You access it by entering an alternative password that you create specifically for access to that hidden volume. This is a password that you would be prepared to withhold much longer than the outer volume password.



VeraCrypt

Slot	Volume	Size	Mount Directory	Type
1				
2	/Users/Silkie/Documents/vera1	1.8 MB	/Volumes/NO NAME	Normal
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

Volume

/Users/Silkie/Documents/vera1

☑ Never save history

1. Create the outer volume

1. Start VeraCrypt and click:'Create Volume' > 'Create an encrypted container' > select 'Hidden VeraCrypt volume' > select the location where the container will be stored on your computer (it can be moved later) and give the container an (innocuous) name. *NOTE: To encrypt an entire external hard drive such as a USB stick, select 'Create Volume' > 'Create a volume within a partition/drive'.*
2. The next screen is titled 'Encryption Options'. The default selections are fine. For the strongest encryption (encrypts multiple times): under 'Encryption Algorithm, select 'AES twoFish-Serpent', and under 'Hash Algorithm', select SHA-512.
3. The next screen is titled 'Volume size'. Select the size of the container (this determines the maximum amount of data that can be put into it).
4. Set the volume password on the next screen. Make a good one (see chapter 8) and Do. Not. Forget!
5. The next screen is titled 'Outer Volume Format'. The program will now generate a random dataset to encrypt the volume. Randomly move your mouse around for a moment, before clicking 'Format'. The program will now create the volume. Depending on the size, chosen encryption algorithm and speed of your computer this will take a few seconds to hours (for very large volumes).
6. The next screen is titled 'Outer Volume Contents' – read this carefully. You must now copy some sensitive looking files into this volume (i.e. copy-paste some files into the VeraCrypt container 'drive' which now appears in My Computer/Finder). Then click 'Next'.
7. The next screen is titled 'Hidden Volume'. Read this, and click Next.

2. Create the hidden volume

Now the outer volume has been created, you will be guided through the creation of the hidden volume. This will take you through the same procedure as in the previous step, but for your hidden volume. You will go through the screens for 'Encryption Options', 'Hidden Volume Size' (the space availability is the size of the outer volume you created minus the size of the files you saved as your decoy in the outer volume), 'Hidden Volume Password' (this *must* be different to your outer volume password) and 'Format Options' (choose FAT).

IMPORTANT: You must choose a different password for the hidden volume to that of the outer volume. It is with these two different passwords that you gain access either the outer or the hidden volume.

3. Put the files you want to encrypt into your hidden volume

Now the volume can be 'mounted' (i.e. activated). Select any slot or drive. Click 'Select File' > locate and select the volume you just made > click 'Mount'.

Now enter *either* the password for the outer or hidden volume, depending on which you would like to access (it should be the hidden volume), and click 'OK'.

NOTE: If you add more data to the outer volume, it may overwrite space/data in the hidden volume. Ideally, you will not change or add any more data to the outer volume after the creation of the hidden volume.

The VeraCrypt container for that volume will now appear on your system as a separate drive (much like a USB drive or external hard disk) and you can put files into it in the same way you would a USB drive (go to My Computer or Finder and click and drag files into the container).

Once you have put the desired files in the container, ‘close’ the container by clicking ‘Dismount’ in VeraCrypt. The container will now appear to be just a file on your computer.

4.2 Encrypting hard drives

Mac and Linux systems

These systems have inbuilt options to encrypt the entire hard drive.

Linux/Ubuntu

You will notice in our guidance on Ubuntu installation (chapter 2), we instructed you to opt to ‘encrypt the Ubuntu installation’ and ‘encrypt the home folder’. These options encrypt the entire hard drive and the home directory with separate passwords.

Mac

Go to System Preferences > Security and Privacy > FileVault > Turn on FileVault.

Windows

The most secure way to encrypt a hard drive on a Windows system is using VeraCrypt.

The method is much the same as those described above, except to begin the process: click 'Create Volume' > select 'Create a volume within a partition/drive' > 'Standard VeraCrypt volume' > Select the hard disk drive.

4.3 Sharing data securely

Risks:

- Interception
- Intervention
- Destruction of source documents
- Identification of source
- Identification of journalist

InfoSec action:

- Exchange encrypted USB drives or hard drives (if you can meet in person)
- Exchange small volumes of data via encrypted attachments with encrypted emails
- Exchange large volumes of encrypted data via a file-sharing service

Physical exchange

The safest way to share large volumes of data is to physically exchange a storage device (ideally a USB drive or hard disk) with the data on it in encrypted form.

The entire device can be encrypted, or several folders stored on the device can be encrypted with separate passwords so that access to them can be given in a controlled manner by the source (who can release passwords over time through secure channels such as encrypted email or OTR-chat – see chapters 5 and 6).

So, all you need to securely exchange data in person is encryption software (such as VeraCrypt) and a USB drive. You can currently buy USB drives with large storage capacity (256GB) for under £30.

Digital exchange

If you cannot physically meet face-to-face with your source to collect the documents, you will need to exchange your documents securely online.

Small volumes of data can be shared as encrypted email attachments, if both of you are using encrypted email (see chapter 5).

Large volumes of data can be encrypted using VeraCrypt, for example, and given an innocuous file name that does not relate in any way to the nature of the data or specifics of the contents. You can then exchange this file via a recommended file-sharing service, and send the recipient a link to the online file and the password(s) to decrypt via a separate, secure channel.

Again, you need a secure system for this to be a safe option. If your hardware or operating system is insecure, the files you exchange and passwords you share may also be insecure – an adversary could potentially have remote access or even control of your computer. Ideally, you will exchange documents between secure systems and both using Tails. For top security, you will only access the documents on an air-gapped machine.

Mega for filesharing

'Mega' (https://mega.co.nz/) is an alternative to popular file-sharing platforms such as Dropbox and Google Drive. Mega runs some encryption inside the browser before the file is uploaded to protect the user against low-level snooping and to legally protect Mega against accusations of facilitating copyright infringement (since they then cannot know the contents of the files being shared). While their encryption should not be considered 'government-proof' it does add a thin layer of protection against snooping on data as it is being transmitted over an open Wi-Fi connection in your chosen anonymous upload café/library. Like most providers of online file storage, Mega will provide 50 GB for every unique email address you have. As with any other aspect of InfoSec, compartmentalisation of data over several accounts that are not relatable to each other is advisable.

SecureDrop

Some journalistic organisations with considerable resources and IT capabilities have implemented their own systems to facilitate the secure sharing of files – notably, SecureDrop. SecureDrop is an open source whistleblower submission system, and it is great news that organisations are using it. However, setting up such systems properly and keeping them secure is not a trivial matter and should not be done without involving specialists with extensive experience and a proven track record. It is not a realistic solution for an independent journalist.

For questions on these matters, contact your organisation's I.T. service provider who may be able to help (but ask them if they have done something like this before, and if not, seek help elsewhere). The CIJ may be able to provide some experienced contacts to get started.

OnionShare:

OnionShare is an open source tool that lets you securely and anonymously (over the Tor network) share a file of any size. It offers a secure method of file-sharing because it allows users to share files directly from computer to computer, across Tor connections, without uploading files to any third party's server. Instead, the sender's computer becomes the server for the purpose of the transfer.

OnionShare is easy to install and use on Windows, Mac, Ubuntu and Tails. Installation on Ubuntu does require minimal use of the command line.

You can download OnionShare and find installation instructions here: https://onionshare.org

To send files using OnionShare, you must have the Tor browser running in the background. You must also use the Tor browser to download files shared via OnionShare.

The sender chooses the files they wish to share, and OnionShare makes the files available for download via a URL, accessible via the Tor browser. As the recipient downloads the file, the sender can see the download progress and completion.

If you are concerned about focused surveillance and attempts to intercept your shared files, you should be careful to share the URL with your contact securely (for example, over encrypted OTR chat or encrypted email) and anonymously (for example, using new anonymous throwaway email accounts created on the Tor browser).

When the download is complete, or when the sender closes OnionShare, the files are completely removed from the internet (unless you untick 'Stop sharing automatically' in OnionShare, which enables the files to be downloaded multiple times).

Further instructions for use can be found here: https://github.com/micahflee/onionshare

4.4 Securely deleting files

On most systems, deleting a file does not actually remove the data from the computer's hard disk (or the USB drive, if that is where it is located). The file still exists but the space it occupies is simply labeled as 'no longer in use', and will eventually be re-used and displaced by other files. However, until then, the 'deleted' files can still be retrieved with the correct forensic tools and expertise.

To securely delete files, you can use specific tools that overwrite files with random data several times. This method is very secure, but may take a significant amount of time for large data volumes (e.g. several hours for multi Gigabyte USB drives).

Windows, Linux/Ubuntu

On Linux and Windows systems BleachBit (http://bleachbit.sourceforge.net/) is the premier open source erasure tool that is considered highly trustworthy.

Tails

The Tails system has a secure erase feature that can be easily accessed by right clicking on a file and selecting 'Wipe'. You can securely delete all 'free' space in a folder by right-clicking on the folder space and selecting 'Wipe available diskspace'.

Mac

- **Securely deleting individual files:**

  The new OS X, ‘El Capitan’, no longer features the ‘Secure Empty Trash’ function due to concerns that secure erasure could not be guaranteed. Therefore, there is now no easy way to securely delete individual files on a Mac, so it is all the more important that you encrypt the hard drive, only allowing access to it with your password.

- **Securely wiping a USB drive (or any external hard drive):**

  Insert the USB drive. Launch ‘Disk Utility’ > select the drive you wish to erase (see menu on the left) > select ‘Erase’ tab. Select ‘Security Options’ and set the slider to ‘Most Secure’ > ‘OK’ > ‘Erase’.

Physical erasure

If an entire disk needs to be wiped there is also the option of physical destruction of the storage device. To be certain that no data can be retrieved afterwards the device needs to be ground up into very small parts no bigger than 1mm. Do not assume that specialised forensic techniques can be defeated by simply breaking a disk with a hammer or immersing the device in water. While this will almost certainly break the functioning of the device, data may still be retrieved if the adversary has the means and time to use advanced methods of data recovery.

Opt for USB drives

Since storing data on the internal disk of a laptop exposes the data to additional risks and possibly makes it harder to securely erase, storing sensitive material on an external storage medium such as a USB drive or external hard disk (for large volumes) is strongly recommended. Encryption of such devices or the files on them is also important to protect against loss or theft by adversaries.

Metadata

Metadata is data about data. Metadata could include the author of a Microsoft Word document, or the GPS co-ordinates of where a photo was taken. Audio, video, and PDF files also hold metadata and hidden data (such as comment or tracking history, file names, etc.). Most colour laser printers print their type and serial number in tiny invisible dots on every square centimetre of paper - so those pieces of paper are traceable if the serial number of the printer is in any way connected to you (e.g. if you ordered the printer online).

Each program used may have specific metadata settings, so you should do some research online (or consult an expert) on whatever program and file you plan to use to be aware of what information is being stored, how you can remove it and how to make sure this information is harmless.

LibreOffice

LibreOffice is a free, open source office suite. https://www.libreoffice.org/

In LibreOffice, user data can be viewed and cleared by going to:

1. File > Properties > General tab

    - Click 'Reset' to reset general user data (e.g. total editing time, revision number)
    - Uncheck 'Apply user data'

2. Then check the 'Description' and 'Custom Properties' tabs and clear any data you don't want disseminated. Under the 'Security' tab, uncheck 'Record changes' if not already clear.

3. Under Edit > Changes > Accept or Reject: you can clear these if the recipient doesn't need them.

4. If you use the Versions feature, go to File > Versions and delete any older versions of the document that may be stored there.

    - (Just for Writer) View > Hidden Paragraphs, check that all hidden paragraphs are visible.
    - (Just for Calc) Format > Sheet, check that there aren't any hidden sheets.

5. Email

Email is very likely the means by which you most frequently contact colleagues and sources. Vitally, it is the means by which a new source could contact you. Therefore, having secure email, not only for everyday use with colleagues but as a secure channel for initial contact, is important for any investigative journalist.

The risks to your email communications include an adversary doing any of the following:

- Reading email content
- Reading subject header
- Seeing who you are contacting, how often and when
- Intercepting email attachments
- 'Man in the middle' attacks (an impersonator intercepting communications)
- Seeing where you are emailing from (location)

InfoSec action:

- Use strong passwords
- Use a trustworthy email provider
- Encrypt your email

- Verify your keys
- Put minimal information in your email subjects
- Email from Tails (if/when you need to)
- Use anonymous email addresses for select purposes

The risks

For protection against most non-state level actors, using a very strong password is a good defence against unauthorised access to your email account. However, for state level actors, it may be no defence at all.

An email provider that is 'trustworthy' is one who has a good basic security infrastructure, and who won't hand over your data to an intelligence agency in a hurry. If you do not trust the country where the email provider is based, it is best not to use an email address there. For example, we know that the default position of the US and UK intelligence agencies is to record and store as many email communications as possible. Even if you don't feel your email communications to be of relevance to these agencies now, they will be retroactively accessible should you and/or your work become relevant in the future. So, if you don't trust the US approach to email privacy, be aware that the email providers based there (Outlook, Gmail, Riseup, etc....) may be subject to that approach.

Some email providers are thought to be more co-operative than others, but unless you run your own server (or the organisation you work for runs their own server in a country with good privacy laws, like Switzerland or Iceland), we should assume that your emails and email metadata are not secure with any email provider. Other considerations are whether you have to hand over your mobile phone number, a postcode/address, or another of your email addresses in order to register an account with a provider, as you may want to avoid donating that information in future (and especially if/when you use an anonymous email address).

5.1 Email metadata

Metadata is data about data. Email metadata includes both the sender's and recipient's names, emails and IP addresses, server transfer information, date, time and time zone, unique identifier of email and related emails, content type and encoding, mail client login records with IP address, priority and categories, subject of email, status of the email, and any read receipt request.

This information is extensive and revealing alone, but many intelligence and law enforcement agencies (and in some cases, individual hackers) are also able to retrieve the full email content.

You can't easily protect the metadata of your emails, so you should be minimalistic or obsfucatory in your subject line, and you may wish to hide your real location/IP address by using the Tor browser.

Example: US government authorities requested access to the metadata of an unnamed user of Lavabit, a secure email provider, as well as the company's private encryption keys (allowing access to user's passwords) in the summer of 2013. Presumably, they asked for this because they were unable to covertly gain access themselves. The attempted breach was thought to be because NSA whistleblower

Edward Snowden had an email account with Lavabit. The founder of Lavabit was legally restricted from discussing the exact requests of the US government – as is anyone approached in this way (which makes evaluating the security of our email providers all the more difficult). Rather than allow a breach of users' privacy, the founder suspended Lavabit altogether, in August 2013.

5.2 Email encryption

However, you can protect the privacy of your email content by using 'public key cryptography'. Public key cryptography scrambles the content of your email into (thus far) unbreakable code using the recipient's 'public key'. The encrypted email can then only be decrypted using the intended recipient's 'private key'.

The following instructions recommend the GNU Privacy Guard, 'GPG' (an open source implementation of Pretty Good Privacy, or PGP).

Using GPG, whilst very different to normal emailing, is not difficult and you will get used to it very quickly. Understanding exactly how it works, however, is slightly more challenging.

Key pairs

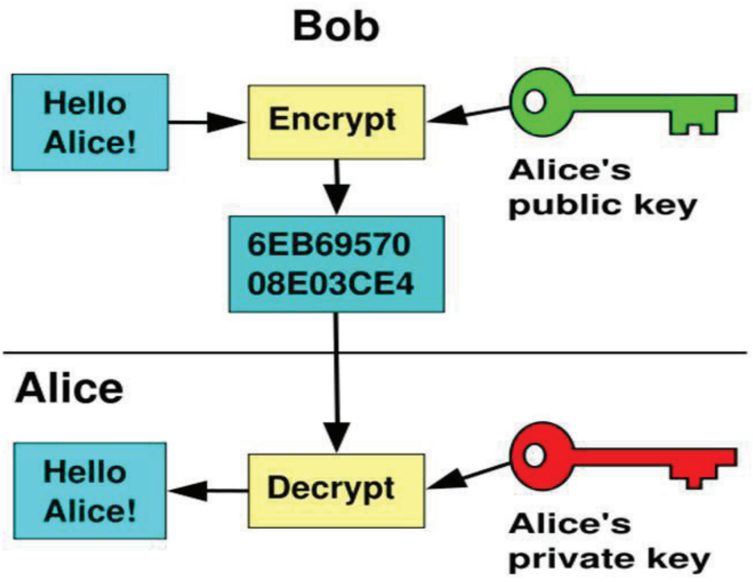
Keys are essentially unique long sets of numbers, and each user of email encryption has a key pair – a public key, and a private key.

- **Your public key:** Your public key is what people will use to encrypt emails that they send to you. Like listing a phone number in the phone book, you can choose whether to list your public key on the public keyserver or not (if it is a secret or anonymous email account, you may not wish to upload the key to the keyserver). If you choose to list your public key on the keyserver, it will be openly available so that anyone can contact you securely.
- **Your private key:** Your private key allows you to decrypt emails from others who have contacted you using your public key. Although your public key is then freely available, the private key in the key pair is exactly that – private! A private key corresponds to your public key, ensuring that no one else can have unauthorised use of your public key. You will probably never even see your private key – it lives and works under the bonnet of your GPG software.

The length, randomness, and sophistication of strong public key cryptography (4096 bit keys, as per our instructions below) are such that the encryption remains, as far as we know, unbreakable.

Verifying keys

Importantly, you should always verify that the keys of the people who you send encrypted mail to really do belong to your intended recipient. Although the email address belongs to the person you want to contact, there is a small chance (at high-risk levels) that their purported public key might not. This is known as a 'Man-In-The-Middle' (MITM) attack – the covert interception of communications by the impersonation of a target. You need to make sure that both the email address and the public key definitely belong to the individual concerned. See 'verifying keys' later in this chapter.



5.3 Protecting your identity and location when emailing

At higher risk levels, for those who wish to hide the real identities of themselves and/or others communicating, anonymous email accounts should be used, unassociated with any other aspect of your online identity - they should not be connected with you in any way. Gmail and Hotmail tend to request a phone or alternate email address, so these providers are not ideal for anonymous accounts. In many countries, GMX and Yandex, allow users to create accounts without such identifying information.

However, if you create an anonymous email address from an internet connection that is associated with you, your anonymity may already be compromised. Furthermore, when you send and receive emails, you are doing so by connecting to the internet – thus your location is known by the internet provider (and potentially, an adversary). If you want your identity and location to be anonymous, you can use an anonymous account to send unencrypted emails through webmail on the Tor browser (see chapter 3); or you can use the Tails operating system, which hides the real location of all of your laptop's communications with the internet (see chapter 2). Tails' desktop email client (which supports encryption) sends and receives information/mail to and from the internet through Tor, thus hiding the real location of the connection.

You might only want to protect your location in the field rather than identity per se. For this, using the Tails operating system is the only answer.

5.4 Basic notes about email encryption

Note that email encryption does not hide metadata such as who you are talking to, the email subject, or your location (though, as discussed, you can hide your real location by using Tor/Tails). For people at all risk levels, it is a good idea to be minimalistic or obsfucatory in your subject line.

You can't encrypt or decrypt email from your smart phone. Whilst it is possible to set up on some Android phones, it is highly inadvisable because mobile phones are fundamentally insecure anyway (see chapter 7).

Neither can you encrypt or decrypt mail in your web browser (unless you are using the Tails operating system) – you will use the Thunderbird email client on your desktop, with the added encryption software, to encrypt and decrypt mail.

Finally, you can only send encrypted emails to other people who also use encrypted email. This used to be a rather small community of people but in a post-Snowden world, it is growing exponentially.

5.5 Installation instructions for encrypted email

Download email client and encryption software

Ubuntu/Linux

For Ubuntu/Linux, use Thunderbird as email client and GPG encryption software. Ubuntu comes pre-loaded with Thunderbird (email client) and GPG encryption software.Use the Ubuntu search tool on the top left hand of the desktop to find it.

Mac

Download Thunderbird email client and GPG encryption software. You will need to download:

- An **email client**/mail manager for your desktop. We recommend Mozilla's open source 'Thunderbird': http://www.mozilla.org/en-US/thunderbird/
- **GPG – Gnu Privacy Guard**, which is encryption software: https://gpgtools.org/. The first pink download box, 'Download GPG suite' will be the latest version – click on it to download. Click on the download when complete, and follow the wizard to install.

When the downloads are complete, open Thunderbird from your Downloads and drag the Thunderbird icon into the Applications folder.

Windows

You will need to download:

- An **email client**/mail manager for your desktop - we recommend Mozilla's open source 'Thunderbird': http://www.mozilla.org/en-US/thunderbird/
- **GPG** – Gnu Privacy Guard, which is encryption software: http://www.gpg4win.org/download.html. The first green download box will be the latest version of GPG – click on it to download. Click on the download when complete, and follow the install wizard to install.

Installation in Ubuntu/Linux, Mac and Windows

On Windows, click on your Thunderbird Setup download. Thunderbird will offer you a brief Setup Wizard – select the standard install, confirm the program file location, and click next to complete and finish the install.

Open Thunderbird. If you are opening Thunderbird for the first time, it may prompt 'Integration' - skip this, and uncheck 'Always perform this check when starting Thunderbird'.

Thunderbird will now prompt you to configure your email account, and offer you a new email address. Click 'Skip this and use my existing email'. Enter the email address you would like to use for encryption and the password. You should decide whether you select 'Remember password' or not. It may be safer if you don't allow your laptop to remember your password, but you will then need to enter the password every time you access the account on Thunderbird. Click 'Continue'. You should see, 'Configuration found in Mozilla ISP database'.

NOTE: If you are using an anonymous email address, obviously, do not enter your real name!

Troubleshooting

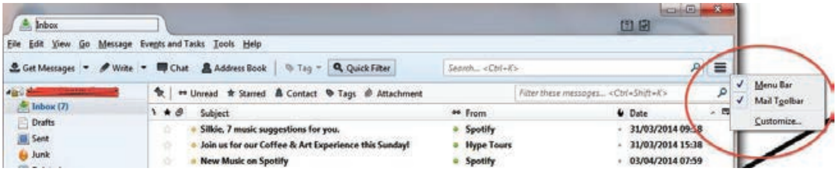
If you receive the error message, 'Configuration cannot be verified', it may be because your email provider uses two-factor verification (e.g. lots of Gmail accounts use '2-step' verification). In this case, you mail provider may email you, or present a web browser, with a notification of an attempted login via a mail client, and ask for your authentication. Alternatively, some Gmail users who use 2-step verification may need obtain an 'application-specific password' – you can do this on the 'authorizing applications and sites' page on your Google Account settings. For more information, visit: https://support.google.com/mail/answer/1173270?hl=en

You now have the option to choose between IMAP or POP3. Choose IMAP if you use webmail, and click 'Done'.

Expert info: Unlike POP, IMAP offers two-way communication between your online email account and your desktop email client – so any changes you make in your email client are communicated back to your online account (e.g. if you mark an email as 'read' on Thunderbird, with IMAP, it will appear as 'read' on your webmail too).

Enigmail security extension

At the top of the Thunderbird window, click on Tools > Add-ons > Extensions. If you see 'Enigmail', you already have Enigmail. If not, go to the search bar in the upper right of the window, and search for 'Enigmail'. Click 'Install', and restart Thunderbird. When Thunderbird restarts, you can close the 'Add-ons Manager' tab.



Subject	From	Date
Silkie, 7 music suggestions for you.	Spotify	31/03/2014 09:58
Join us for our Coffee & Art Experience this Sunday!	Hype Tours	31/03/2014 15:38
New Music on Spotify	Spotify	03/04/2014 07:59

NOTE: if you do not have a menu bar at the top of the Thunderbird window, right-click on the 3-line menu icon on the top right hand side of the Thunderbird window and tick 'Menu bar'.

Key pairs

At the top of the Thunderbird window, click on Enigmail > Key Management. Back up to the top toolbar, click > Generate > New key pair

- The email address you wish to use for encrypted mail should be selected
- Tick 'Use generated key for the selected identity'. Select key to expire in 5 years
- Enter a passphrase (this is the passphrase for your encrypted mail – not just your online mail account – it should be very strong)
- The 'Comment' box adds a public comment to your public key if you list it on the keyserver (so don't use this for a password hint!)
- Under 'Key expiry', the Key should expire in 5 years
- Click the 'Advanced' tab, and select the maximum key size of 4096, and Key type 'RSA'
- Click 'Generate key' and move your mouse around the screen whilst it generates your key (this aids the 'randomness pool' from which the key is configured). This may take a few minutes.
- A box will appear informing you that the key generation is completed.

Click 'Generate Certificate' in this box (this creates a revocation certificate that you will need when you wish to invalidate your key, for example, if the key pair is lost or compromised). Save the revocation certificate somewhere safe. You will now be asked to enter your passphrase in order to complete this action.

Configuring Thunderbird

Go back into Thunderbird to change some settings.

Expert settings

Enigmail > Preferences > Display Expert Settings

- Basic > Passphrase settings: here you should select how long you want Thunderbird to remember your key pair passphrase for
- Sending: Select 'Manual encryption settings' and tick:

    - 'Encrypt/sign replies to encrypted/signed messages'
    - 'If possible', under 'Automatically send encrypted'
    - All usable keys', under 'To send encrypted, accept'; or tick 'Only trusted keys' if you are able to carefully check contacts' keys and set trust levels from the beginning of your encrypted communications with them.'Always', under 'Confirm before sending' N.B. this is a very useful tool that tells you every time you send an email whether the email is signed and encrypted so you are much less likely to accidently send an unencrypted email

- Key Selection: Tick 'By Per-Recipient Rules', 'By Email Addresses according to Key Manager', and 'Manually if Keys are Missing'

- Advanced: we recommended that you tick ‘Re-wrap signed HTML text before sending’ as HTML text does not work well with encrypted emails.

Click ‘Ok’.

Saving folders locally

This is particularly useful for saving drafts – you don’t want your draft, unencrypted emails being saved on your online mail folders. Rather, you should save them locally on your hard disk to have more control over their security.

In the menu bar on the left hand side of the Thunderbird window, you will see all your email folders. At the bottom, are ‘Local Folders’ – right click and select ‘New Folder’. Creating ‘Sent’ and ‘Draft’ local folders may be helpful.

Click Edit (Linux) or Tools (Mac/Windows) > Account Settings > Copies & Folders. You can select where to store your messages here. For example, under ‘Drafts and Templates’, select ‘Local Folders’ as the location to keep your message drafts.

In the same window [Edit (Linux) or Tools (Mac/Windows) > Account Settings] click OpenPGP Security > tick ‘Encrypt draft messages on saving’.

Email in plain text

HTML does not encrypt well, so you will write messages in plain text instead.

Edit (Linux) or Tools (Mac/Windows) > Account Settings > Composition & Addressing. Untick ‘Compose messages in HTML format’

Share your PGP signature with contacts

You should always sign encrypted messages to help the recipient verify that you are the real sender. Sharing your PGP signature with the people you email, even when the email is not encrypted, also helps the recipient (if they also use Enigmail) verify that you are the real sender of the message (not an impersonator). If the recipient does not use PGP encryption, signing unencrypted mail indicates that you usually use PGP encryption – or to the uninformed, it may be mildly confusing!

Edit (Linux) or Tools (Mac/Windows) > Account Settings > OpenPGP Security ‘Enable OpenPGP support (Enigmail) for this identity’ should be ticked.

Tick ‘sign encrypted messages by default’. If you wish, you may select ‘Sign non-encrypted messages by default’ – when you sign a message, whether encrypted or not, it helps the recipient (if they also use Enigmail) verify that you are the real sender of the message (not an impersonator). Click ‘OK’.

Publicly list your public key

Uploading your public key to the keyserver is like listing your phone number in a phonebook. It allows people to search for your name/email address, and locate your public key in order to send you an encrypted email. This is very useful for journalists who invite encrypted mail and wish to protect source confidentiality. However, if you are setting up encryption for an anonymous email address that you will use only to communicate with specific, high risk individuals, of course there is little to gain from uploading your public key to the keyserver.

Enigmail > Key management

Tick ‘Display All Keys by Default’. Right click your email address, and select ‘Upload Public Keys to Keyserver’ if you want people to be able to contact you. The default keyserver (pool.sks-keyservers.net) is fine.

To search for anyone’s public key

Search for a name/email address to see if a person has a public key listed, so you can send them encrypted mail (like searching for a number in a phonebook).

Enigmail > Key management > Keyserver (in the top toolbar) > Search for keys. Enter the person’s name or email address and browse the results. Tick the email address of anyone whose key you’d like to import and press ok.

Import a key

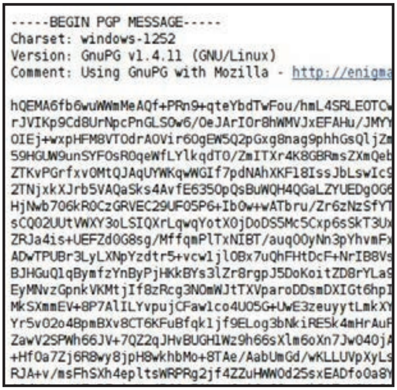
If you already have your contact's key on a file or online, but need to import it to your key manager on Thunderbird.

Importing a key from file: In Thunderbird, go to Enigmail > Key management. Now go back up to the top toolbar to click on File > Import keys from file.

Importing a key from email: If your contact has attached their public key in an email, right-click on the .asc attachment and click 'Import OpenPGP Key'. The attachment may look like:

1 attachment: 0xA332E5DB.asc

Importing a key from a public key block: Many people have their full public key 'block' (i.e. the full public key in text) on their website. This allows people to trust the website as the source of the key rather than the keyserver, and may help prevent man-in-the-middle attacks. Simply copy the whole key block (the entire block, as shown highlighted in yellow below), then in Thunderbird go to Enigmail > Key management > (back up the top toolbar) Edit > Import keys from clipboard > click 'Import' in the confirmation box.



```
-----BEGIN PGP MESSAGE-----
Charset: windows-1252
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigma

hQEMA6fb6wuWWmMeAQf+PRn9+qteYbdTwFou/hmL4SRLEOTC
rJVIKp9Cd8UrNpcPnGLSOw6/OeJArIOr8hWMVJxEFAHu/JMY
OIEj+wxpHFM8VTOdrAOVir6OgEW5Q2pGxg8nag9phhGsQljZm
59HGUW9unSYFOsROqeWfLYlkqdTO/ZmITXr4K8GBRmsZXmQeb
ZTKvPGrfxvOMtQJAqUYWKqwWGIf7pdNAhXKF18IssJbLswIc
2TNjxkXJrb5VAQaSks4AvfE635OpQsBuWQH4QGaLZYUEDgOG
HjNwb7O6kROCzGRVEC29UFO5P6+IbOw+wATbru/Zr6zNzSfYT
sCQO2UUtVWXY3oLSIQXrLqwqYotXOjDoDS5Mc5Cxp6sSkT3U
ZRJa4is+UEFZdOG8sg/MffqmPlTxNIBT/auqOOyNn3pYhvmF
ADwTPUBr3LyLXNpYzdtr5+vcw1jlOBx7uQhFHtDcF+NrIB8Vs
BJHGuQlqBymfzYnByPjHKkBYs3lZr8rgpJ5DoKoitZD8rYLa
EyMNvzGpnkVKMtjIf8zRcg3NOmWJtTXVparoDDsmDXIGt6hpI
MkSXmmEV+8P7AlILYvpujCFaw1co4UO5G+UwE3zeuyytLmkX
Yr5vO2o4BpmBXv8CT6KFuBfqkljf9ELog3bNkiRE5k4mHrAu
ZawV2SPWh66JV+7QZ2qJHvBUGH1Wz9h66sXlm6oXn7Jw04OjA
+HfOa7Zj6R8wy8jpH8wkhbMo+8TAe/AabUmGd/wKLLUVpXyLs
RJA+v/msFhSXh4epltsWRPRg2jf4ZZuHWWOd25sxEADfoOa8Y
```

Verifying keys

Make sure that the person you think you are communicating with is certainly who they say they are.

In Thunderbird, go to Enigmail > Key management > right-click a selected email address > Key Properties. Here you will see the person's key ID and fingerprint.

You can verify that the key does indeed belong to the person by exchanging fingerprints by another communication means (in person, on the phone, on their business card/website), and checking they match exactly. In the same window you can then click Select Action > Set Owner Trust > and select how much you trust that the key does in fact belong to the individual concerned.

Add a regular email signature

With your name, job title, website, email address/es, PGP fingerprint, etc...

- Edit (Linux) or Tools (Mac/Windows) > Account Settings Here you can enter signature text to attach to your emails.
- Edit (Linux) or Tools (Mac/Windows) > Account Settings > Composition & Addressing
- Select 'Include signature for replies'

Receiving new mail

You can decide how frequently the mail client searches for new messages.

- Edit (Linux) or Tools (Mac/Windows) > Account Settings > Server settings

Send an encrypted email!

When you have completed the set up, send a test email to someone else who has encrypted mail. Import their key or find it on the keyserver, and be sure to verify it and sign your trust of their key before you try to send an email (otherwise the email client might not actually let you send them encrypted mail – Thunderbird will encourage good InfoSec in this way!).

Choose a recipient whose key you have already imported, verified, and set owner trust for. Write your email, and before you click 'Send', either click on the padlock icon to close it and encrypt the message, or go to 'Enigmail' within the email compose window and click on 'Encryption Off' to turn the encryption on. Press 'Send', and the confirmation box should tell you that the email is both signed and encrypted (if not, go back and check you ticked to encrypt). Click 'Send Message', and your encrypted email will be sent!

Now that you have sent this person an encrypted email, a default setting should be created whereby all future emails to this contact will automatically encrypt.

Share your public key with an individual

The first time you send a contact an encrypted email, you should attach your public key so that they can respond by encrypting an email back to your key. In the email compose window, to the right of the encryption padlock and signing pencil icons, there is an option to 'Attach My Public Key'. Select this to attach your public key to the email. Alternatively, click 'Enigmail' > 'Attach My Public Key'.

Sending/receiving attachments

You can encrypt and decrypt attachments to your emails with GPG too

When sending a file as an attachment to an encrypted email, you can choose whether or not to encrypt the attachment too. Write the email, attach a file as normal, and click 'Send'. Before the email sends, you will be given four options. The first option is to just encrypt the message but not the attachments. The second is to encrypt the message, and to also individually encrypt attachments. Opt for the second choice ('Encrypt and sign each attachment separately and send the message using inline PGP'), and click OK. Then your confirmation box will pop up as usual, telling you the message and attachments are signed and encrypted – click 'Send Message' to confirm, and the email and attachment will be sent.

When someone sends you an encrypted email attachment, right click the attachment and click 'Decrypt and Save As'. Save it in your chosen location, and then go to that location to find/open the attachment.

Of course, if you are mailing an attachment that has already been encrypted by other means (e.g. VeraCrypt), you don't need to encrypt it again using GPG.

Add a new account

You may wish to add another email account to Thunderbird, whether you intend on using encryption on that account or not.

In Thunderbird go to Tools (or 'Edit' on Linux) > Account Settings > Account Actions > Add mail account.

6.

Instant Messaging

Instant messaging is a great way to start and maintain conversations with a source. It is very quick and easy to set up encrypted, ‘off-the-record’ (OTR) instant messengers (IM) – especially compared to setting up encrypted mail. Using an OTR IM, you can discuss necessary security protocols before you continue conversing, meeting, emailing, sharing documents/ information, and so on. It is also a useful tool for talking to colleagues if you are collaborating remotely on a project. However, we strongly recommend not using smartphones for chatting from risk level medium and up because their safety can never be guaranteed.

Off-the-record instant messaging allows you to have private conversations that are not only encrypted, but that are not stored, and therefore ‘deniable’. That is to say, it is plausible that a chat purportedly including a chat account associated with you, is not actually you.

Expert info: Like encrypted emailing, OTR IM uses public keys that are used to verify a contact really is who they purport to be. However, every time you begin a new chat with a contact (who has been verified by their public key), the chat is encrypted using new, throwaway keys. Don’t worry – you don’t have to do or even see this yourself – this is under-the-bonnet encryption that the messenger client does it for you.

6.1 Pidgin and Adium

If you are using Linux or Windows, we recommend that you use an IM client called Pidgin, with an OTR plug-in. If you are using Mac, we recommend an IM client called Adium.

Users of Pidgin and Adium can communicate easily with one another. However, in the current versions, the verification methods for the two messenger clients are different. See 'Verifying contacts'.

Pidgin instructions for Linux (Ubuntu)/Windows

1. **Download Pidgin and OTR plug-in**

Pidgin and OTR are often included software in Linux distributions, so simply search in your Ubuntu (or other Linux distribution) Software Centre.

Download and install Pidgin at https://www.pidgin.im (Windows); if you're on Ubuntu, you will be directed from that page to the Pidgin PPA package, so download that.

For Windows, then download the OTR plug in from: https://otr.cypherpunks.ca. On Ubuntu, go to the Ubuntu Software Centre, search for Pidgin OTR, and install the 'Pidgin Internet Messenger Off-the-record Plug-in'.

2. Configure Pidgin

Open Pidgin. If this is the first time you are opening Pidgin, you will not have an account configured and will be prompted to 'Add an account'. Click 'Add' (if you are not prompted, you can find this at Accounts > Manage Accounts > Add).

- First, you may wish to configure Pidgin to only connect your IM account via Tor, thus shielding your real location – particularly useful if you want to use the account anonymously. Under the 'Proxy' tab, tick 'Connect using proxy' and choose 'SOCKS5' from the dropdown list. In the Server field type '127.0.0.1' and in the Port field type '9150'. *The username and password fields are optional, but if you use them Tor will use different circuits for this account in Pidgin than it will for everything else, increasing your anonymity. Note that you will now need to have the Tor browser open (see chapter 3) in the background when you wish to connect with this account.*
- In the 'Basic' tab, select XMPP/Jabber (NOT Facebook XMPP) under 'Protocol' and choose an (anonymous) username. Under domain, type your selected domain (for example, jabber.ccc.de) – see a full list of domain options here : https://list.jabber.at. In the 'Resource' field, type 'anonymous'. Make a strong password
- Click on the 'Advanced' tab and for 'Connection security', ensure 'Require encryption' is selected
- Click back on the 'Basic' tab and be sure to tick 'Create this new account on the server' (bottom of the window) before you click 'Add'

3. Create an IM account

Your Jabber address should appear in an 'Accounts' window. Tick the 'Enabled' box and then click 'register' in the 'Register New XMPP Account' window that appears.

4. Configure OTR

In Pidgin, go to Tools > Plug-ins > tick 'Off-the-record messaging'. Then click 'Configure plug-in'. Tick all the default OTR settings: Enable private messaging; Automatically initiate private messaging; Require private messaging, and Don't log OTR conversations. Now click 'generate' to generate a key for your account.

Go to Tools > Preferences > Logging, and untick all logging options.

Congratulations! You can now enjoy off-the-record, encrypted chat.

Adium instructions for Mac

1. Download Adium

Download and install 'Adium' for Mac – https://adium.im/

2. Create and configure an IM account.

Once downloaded, open Adium and go to (at the top) 'File' > 'Add account' > 'XMPP'.

- First, you may wish to configure Adium to only connect your IM account via Tor, thus shielding your real location – particularly useful if you want to use the account anonymously. Under the 'Proxy' tab, tick 'Connect using proxy' and choose 'SOCKS5' from the drop-down list. In the Server field type '127.0.0.1' and in the Port field type '9150'. The username and password fields are optional, but if you use them Tor will use different circuits for this account in Adium than it will for everything else, increasing your anonymity. Note that you will now need to have the Tor browser open (see chapter 3) in the background when you wish to connect with this account.
- In the 'Account' tab choose an (anonymous) name and add a domain at the end of it for your Jabber ID (for example, @jabber.ccc.de is popular – see a full list of options here https://list.jabber.at). A full Jabber ID may be, for example, kissinger@jabber.ccc.de. Under 'password', choose a strong password. Do not 'register account' yet.
- In 'the Options' tab tick 'Require SSL/TLS' and tick 'Do strict certificate checks'. Under 'Resource', type 'anonymous'.
- In the 'Privacy' tab and in the 'encryption' drop down menu click on 'Force encryption and refuse plain text' (last one on the list)
- Go back to the Account tab and click 'register account'. A new window appears: in 'server', type the domain you previously selected (e.g. 'jabber.ccc.de' if you went for that) then click 'Request new account'. In a moment, your account should be successfully created.

3. Configure Adium

Go to Adium > Preferences > General > untick 'Log messages'

6.2 Getting started with OTR chat

Add a contact

- **Pidgin:** In Pidgin, go to Buddies > Add a buddy and type in their full address before clicking 'Add'. When your contact is next online, they will receive an authorisation request from you. To start a conversation with an online contact, double click on a buddy/contact in your list, and click OTR > 'start private conversation' in the chat window.
- **Adium:** In Adium, go to Contact in the top toolbar > Add contact. Under 'Contact type', assuming your contact is also using Jabber, select XMPP/Jabber, enter their full address in 'Jabber ID', and click 'Add'.

Authenticating/verifying a contact

Ideally, you will use fingerprint verification and if you know the person well enough, you will also ask a question of each other, that only the other person would know the answer to.

- **Pidgin:** If you have not yet authenticated your contact, double click on their address to open a chat window with them, go to OTR in the chat window and click 'Authenticate buddy'. You can authenticate either by

    - A question and answer - A good, personalised method
    - A shared secret - Has to be pre-arranged via a different communication method

    - Manual fingerprint verification. - A useful and strong method, - The only method by which Adium and Pidgin users can authenticate one another. In that window, select ‘Manual fingerprint verification’ as the method, and you will then see your contact’s purported fingerprint. Check the fingerprint – if it is ok, select ‘I have’ verified that this is in fact the correct fingerprint, and click ‘Authenticate’.

- **Adium**: If you have not yet authenticated your contact, double click on their address to open a chat window with them (even if they appear to be offline – they will appear offline and ‘not authorised’ until you verify them). Click the lock icon and select ‘Initiate Encrypted OTR chat’. The lock should close. With the chat window still open, go to the top toolbar in Adium, click Contact > Encryption > Verify. You will then see your contact’s purported fingerprint.

Checking fingerprints

You should ideally check one another’s fingerprints by a communication method other than IM (email, phone). If there is not a secure means by which to do this, a mutual friend/third party on IM can pass on a partly redacted version of your fingerprint to the contact (e.g. 0---A7-0 D—706-D 2—65--1 --3D-9C2 0-57B—1), and the contact’s fingerprint to you, for you both to check alongside the purported fingerprint shown. Redacting parts of your fingerprint may help prevent a ‘man-in-the-middle’ impersonation attack.

Finding your own fingerprint

Adium users can find their own fingerprint in Adium > Preferences > Advanced (horizontal tab) > Encryption (tab on the left hand side column).

Pidgin users can find their own fingerprint by opening a chat window with a contact, clicking the small buddy icon (right of 'OTR') > Re/Authenticate buddy > Manual fingerprint verification.

NOTE: do not allow Adium or Pidgin to automatically remember your Jabber password, as it may not be saved securely.

7.

Phones and Voice/Video Calling Over Internet

7.1 Mobile security

Many of us find our smart phones to be of great importance and value in our everyday lives and work. The benefits of being constantly connected to our email accounts, web browsers, social media, calendars, and also having easy access to a high quality camera and voice recorder, do indeed make them valuable tools. However, they are not feasibly securable tools.

An alternative is to use burner phones, with diligence and caution – but even this has its risks.

Phone risks:

- Automatic logging of your current/past locations
- Automatic collection of metadata, i.e. the phone number and location of every caller; unique serial numbers of phones involved; time and duration of call; telephone calling card numbers
- Theft and loss of data
- Remotely accessing data when phone connects to public Wi-Fi

- Remotely accessing all data at any point the phone is on
- Phone/voicemail tapping, intercepting, or recording
- Covert remote automation of microphone to record audio
- Covert remote automation of camera to capture images

Dragnet phone surveillance

All phones leak an enormous amount of information about us to intelligence agencies, and we know from the Snowden revelations that programs collecting the full audio of every single call within a nation are, at the very least, already being trialled in some countries. This type of surveillance is extremely dangerous for democracy, let alone journalism, and may permit the most invasive 'retroactive' investigation of individuals who become of interest to intelligence agencies at some point in the future.

Therefore, it is worth using any phone with this in mind, whether you, your sources or colleagues may be targets of intelligence agencies now, or years in the future. They are not secure communication devices, so consider carefully how you want to use them.

Targeted phone surveillance

Low risk

At a low risk level, the threat is mainly physical – someone gaining access to the handset. If this happens, even a fairly unsophisticated hacker/the police can normally crack your password (if you use a password lock) so this only provides minimal protection. If you are at a low risk level, be sure to back up your data and stream or send any video or audio being recorded on the device to a secure storage cloud as soon as possible.

You can also use applications to track your device, should it be stolen. For iPhone, for instance, Apple offer a free app called 'Find my iPhone' which tells you the current location of your phone. Another free anti-theft app is 'Prey' which, once you report the phone as stolen, will record not only the current location of the phone, but any other locations of the phone registered since you reported it stolen.

Medium risk

At a medium risk level, you may encounter an adversary trying to gain access to your data, not just physically, but remotely. When you connect a phone to a public Wi-Fi connection, for example, a fairly unsophisticated hacker can intercept lots of information about you and connected accounts such as email and social media. Therefore, at a medium risk level, you may already be thinking about avoiding a smart phone as a work tool, or at least guarding it closely, closing applications after use, turning off Wi-Fi in public, and using flight mode when you don't need to be connected.

A NOTE ABOUT SMARTPHONES: the vulnerabilities of smart phones are numerous, with some existing in the hardware, and they are not fixable. You can use open source software on smart phones, and even applications for encrypted chat (e.g. Signal). However, as we discovered in 'Protecting the System', when hardware is vulnerable, the software cannot provide you with real security. Therefore, we will not discuss such apps for the purpose of this guide.

As the recent phone hacking scandal in the UK demonstrated, unsophisticated hackers working for unethical journalists were able to listen in on people's voicemail. Private investigators often also have the ability to 'phone tap' (i.e. eavesdrop) not only voicemail but general phone calls made and received by a number. Therefore, you should think before you discuss anything sensitive on your (mobile or indeed landline) phone.

High risk

At a high risk level, a phone basically is your adversary. At the very least, it logs your location, and all associated metadata with the device is in the hands of a Five Eyes intelligence agency. At worst, it can be exploited to covertly collect the content of all of your phone calls, let alone all other data on the phone, and to covertly automate your microphone and camera to record audio and images (if it has a camera) too. This type of phone surveillance is very easy and basically comes at zero-cost to Five Eyes intelligence agencies.

Burner phones

An alternative way of using phone communications is to use burner phones.

Ideally, your burner phone and regular phone will never both be emitting signals, since (if you are a target), your regular phone may pick up on the signal of the burner phone, making that a target too.

Before you use a burner, make sure the phone usually associated with you (e.g. your smart phone) is not emitting signals. Switching the phone to flight mode, removing the battery (don't bother trying to do this to the iPhone), and turning it off is good but is not enough. Do all of these things and then put it in a Faraday cage – popular solutions are biscuit tins, some fridges, or even a stainless steel cocktail shaker! The phone has to be completely sealed in metal (check it is working by trying to call the phone). It is a good idea to find and carry a small tin around with you to put your phone in, and in an important meeting, make sure all attending have done the same (a larger biscuit tin works well here!).

A burner phone is a cheap, cash-bought, throwaway, low-tech phone, with a prepaid SIM card not registered to you, to be used only for specific purposes. It can be hard, in some countries, to buy a SIM card without registering it with your personal details. Therefore, buying second-hand, or having a contact that can obtain such SIM cards, is ideal.

After some use of the phone, the phone may become associated with you and attract surveillance, at which point you should destroy it and use a new one. Changing the SIM card is not enough – each phone handset also has an IMEI (International Mobile Equipment Identity) number that identifies the phone. If the SIM has been identified as being yours, the IMEI will be too – so you will need to destroy the phone.

Due to intelligence agencies rolling out full audio recording of all phone calls, let alone the ease with which they can record a target's phone calls, you should avoid sharing particularly sensitive information - even on a burner phone.

WARNING: intelligence agencies are increasingly developing methods to identify use of burner phones, by scanning bulk communications data patterns for anomalies. It is thought that they similarly surveil use of public phone booths. Therefore, one should conduct a risk assessment before using burner phones to communicate with a high-risk source.

7.2 Internet voice and video calling

Software that provides voice and video calling over the internet (Voice over Internet Protocol, VoIP), such as Skype, is enormously popular and useful, with Skype having over 700 million users itself. However, Skype does not offer much security, and there is not yet any user-friendly, secure alternative.

Among the Snowden revelations are details of the NSA's ability to intercept and store Skype communications. We should assume that all Skype communications are not just between us and our contacts, but with intelligence agencies too.

EXAMPLE: Glenn Greenwald tells a story of when he used Skype in Hong Kong to call his partner back in Rio, David Miranda, to tell him he would receive some encrypted documents by email, and to store them securely. Greenwald never did send those files – but 48 hours later, Miranda's laptop was stolen from their Rio home.

We should also assume that it is not only the most sophisticated agencies that have covert access, or who have exploited security flaws. For example, Egypt's secret police are known to have purchased Skype penetration tools, and man-in-the-middle Skype attacks have been reported by environmental campaigners working in Asia.

8.

Passwords

All of the systems and tools in this book use passwords as a method to correctly identify authorised users and secure against unauthorised access. Strong passwords are a key line of defence at all levels of information security.

However, bear in mind that passwords to online accounts are mainly a defence against non-state hackers (who are also able to obtain increasingly sophisticated commercial password cracking programs). There may be backdoor access at a state level to your online accounts, ultimately rendering a password irrelevant. That is one good reason to encrypt your emails – you may have an incredibly strong Hotmail password, but it doesn't stop intelligence agencies forcing Hotmail to handover all of your emails anyway (or more likely, covertly intercepting and collecting them without permission). If your emails are encrypted, all Hotmail can hand over is a pile of (thus far) uncrackable code.

So, whilst strong passwords are always a good idea, passwords that protect your system (e.g. hard disk encryption) and your encryption programs are far more important than passwords to online accounts.

Risks:

- Forgetting and losing passwords
- Overriding passwords by backdoor access (online accounts)
- Hacking (relatively unsophisticated password hacking)
- Password cracking (sophisticated)
- Key logger
- Being coerced into revealing a password

InfoSec action:

- Learn how to create strong passwords
- Use KeePassX password manager (if you trust your system). KeePassX is an open source password manager that can generate and store usernames and passwords in an encrypted, local database, protected by your master password. It is available for Linux, Mac and Windows.
- Store the most important passwords in your head only
- Use hidden volumes for important encrypted files

8.1 Password cracking: understanding the risk

If your system is insecure, password cracking in a targeted attack is simple. An adversary could physically or remotely insert a key logger into your system, to record every keystroke. This would mean that an adversary captures every thing you type, including your passwords. This is not a hugely sophisticated attack and yet totally invalidates other security measures. Therefore, it really is important to secure your system in the very first instance, as described primarily in chapters one and two.

However, if your system is secured and your adversary does/can not use key logging tools, an attacker may try to crack the passwords that protect your system, software and accounts (and this may be either in a large scale hack of thousands of users, or in a targeted attack against an individual).

Password cracking programs are used by authorities across the world, but sophisticated versions are also available as commercial products. A password cracker can automatically test at least eight million passwords per second and may run for days, on many machines simultaneously. For a high-profile target, a password cracker could run on multiple machines, for months.

Password crackers try the most common passwords first. A typical password consists of a root plus an appendage. The root isn't necessarily a dictionary word, but it's usually something pronounceable. An appendage is either a suffix (90% of the time) or a prefix (10% of the time). A cracking program would typically start with a dictionary of about 1,000 common passwords, such as "letmein," "temp," "123456," and so on, and then test them each with about 100 common suffix appendages: "1," "4u," "69," "abc," "!," and so on. It is thought that about a quarter of all passwords can be cracked with just these 100,000 combinations.

Crackers use different dictionaries: English words, names, foreign words, phonetic patterns and so on for roots; two digits, dates, single symbols and so on for appendages. They run the dictionaries with various capitalisations and common substitutions: '$' for 's', '@' for 'a', '1' for 'l' and so on. This guessing strategy quickly breaks about two-thirds of all passwords.

The attacker can feed any personal information available about the password creator into the password crackers. A good password cracker will test names and addresses from the address book (post codes are common appendages), meaningful dates, and any other personal information it has.

A particularly comprehensive attack can be launched if your hardware is insecure (the root of all problems!). An attacker can index a target's hard drive and create a dictionary that includes every printable string, including deleted files. If you ever saved your password in an obscure file somewhere, or if your program ever stored it in memory, this process will grab it and aid the process of cracking your password.

8.2 How to create a strong password

A strong password is one that the cracking process described will miss.

Password manager

One option is to use open source password management software such as KeePassX to generate a random, long, alphanumeric password (with symbols too, if they are permitted for the particular password), and then save it in your own encrypted password database. If you trust the other layers of your system, this is a fairly robust option.

Furthermore, this is a good way to store multiple complicated passwords for multiple accounts, with KeePassX also having entry fields for URLs, account names and comments for each password stored, so you can securely store all the information you need. The random passwords generated are unmemorable, which fulfils a security function in itself. However, KeePassX allows you to easily copy and paste passwords from the database, so you don't even have to type them.

There is some debate as to how good such programs are at effectively randomising, but the human brain is pretty awful at randomising too, so it remains one of the best options we currently have.

You will need to create a master password for KeePassX, which must be very strong. You should aim to store this password only in your own head.

Schneier scheme

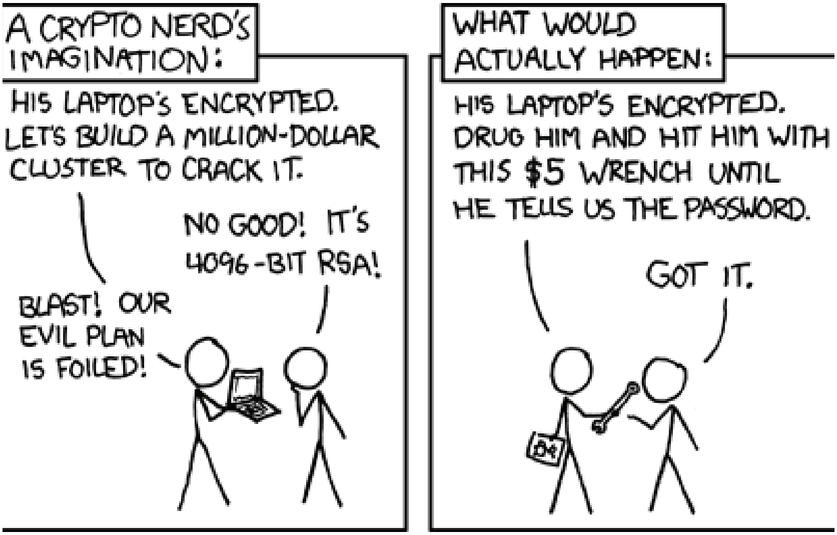
You should use manually created passwords to encrypt your whole system, any encrypted USB stick or highly important file (e.g. source documents), and your password manager. These important passwords should be stored in your human memory only, and therefore need to be memorable.

Of course, to minimalise any damage should a password be compromised, you should avoid re-using passwords.

To manually create a password, we recommend the 'Schneier scheme', a method advocated by Bruce Schneier, the internationally renowned cryptographer and security expert.

Schneier advises taking a memorable sentence and initialising, symbolising, and numbering the words to turn it into a password.

For example, “This little piggy went to market” might become “tlpWENT2m”. That nine-character password won’t be in anyone’s dictionary. Choose your own sentence - something personal, but not obviously related to you through public data.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Here are some examples:

- **WIw7,mstmsritt...** = When I was seven, my sister threw my stuffed rabbit in the toilet.
- **Wow...doestcst** = Wow, does that couch smell terrible.
- **Ltime@go-inag~faaa!** = Long time ago in a galaxy not far away at all.
- **uTVM,TPw55:utvm,tpwstillsecure** = Until this very moment, these passwords were still secure.

Of course, do not use any of the above examples – now that they have been used, they are invalid as strong password options.

8.3 Being coerced into revealing a password

Let's hope that you are never in this situation. However, let's say a malicious group or agency has intercepted you, carrying an encrypted USB stick (with your most important files, or source documents), and they are prepared to go to extreme lengths to obtain the password in order to decrypt. What do you do?

In these instances, it may be helpful to have a hidden volume on your USB drive. A hidden volume is not visible to anyone and does not appear to take any space on a drive. As such, it can be overwritten easily. However, it means that the visible encrypted volume can act as a decoy, and provide you with plausible deniability. In the visible encrypted volume, you can store files that could reasonably warrant security and encryption, and this volume has its own password. However, the hidden encrypted volume sits undetected beneath the visible volume, and has a separate password.

You can create a hidden encrypted volume with VeraCrypt (see chapter 4). This method may help protect the information from interception, but not from loss – it can be easily destroyed or overwritten so you should always back up important files.

Much of this chapter is adapted from Bruce Schneier's blog: https://www.schneier.com/. We thank Mr. Schneier for allowing us to use his work.

Glossary

AMT chipset Chipset with Intel Active Management Technology for automated management (vulnerable than older chipsets from before 2008)

Air-gapped A security measure whereby a laptop is kept entirely offline, separate from other local networks and the internet

Backdoors Covert security vulnerabilities that allow a system's known security mechanisms to be bypassed, allowing undetectable access to the computer or its data

BIOS Basic Input/Output System - a set of computer instructions in firmware that control input and output operations

Bridges (Tor) Bridges are Tor relays (nodes or computer points that receive traffic on the Tor network and pass it along) that help circumvent censorship

Dragnet A mass surveillance system operated through programs that sift through and collect the world's online and telecommunication data

Faraday cage	A metallic enclosure that prevents the entry or escape of an electromagnetic field
Firmware	Software programmed onto hardware that provides instructions for how the device communicates with the other computer hardware (includes BIOS)
Hardware	The physical elements that comprise a computer system
Malware	Malicious software, typically spyware, designed to disrupt or damage a computer system
MITM	Man-in-the-middle attack: The covert interception of communications by the impersonation of a target
Metadata	Data about data
Middleware	Programming that “glues” together”/mediates between two separate and often already existing programs: e.g. allows programs to access databases
Open source	Freely distributed software for which the source code is publicly available

Operating system The software that takes control of the computer as it boots up, tells the computer what to do and how to do it, and is the interface through which you use the computer

Tor network Worldwide network of computers , called Tor-nodes

Tor relay Nodes of computer accesspoints that receive and pass on traffic

About the authors

Silkie Carlo is the director of Big Brother Watch. Before joining Big Brother Watch, she was the Senior Advocacy Officer at Liberty where she led a programme on Technology and Human Rights and launched a legal challenge to the Investigatory Powers Act. She previously worked for Edward Snowden's official defence fund and whistleblowers at risk.

She is a passionate campaigner for the protection of liberties, particularly in the context of new and emerging technologies. She has worked to uphold rights in the fields of state surveillance, policing technologies, big data, artificial intelligence and free expression online. Silkie is also an information security trainer and organises 'Cryptoparty London'. She is the co-author of Information Security for Journalists.

Arjen Kamphuis was co-founder and Chief Technology Officer of Gendo. Kamphuis studied Natural Sciences at Utrecht University. Since 2006 he helped to secure the information systems of corporates, national government and NGO's. His work ranges from regular privacy-compliance and security-awareness up to countering espionage against companies, journalists and governments. He worked on the strategic impact of new technological developments and the social, economic and geo-political impact of science and technology. Since 2009 Arjen has been training journalists, politicians, lawyers, human rights workers and whistleblowers to defend their communications and data from government or corporate intrusions or manipulation.

If you would like to offer any feedback about this InfoSec book, we would be most grateful to receive it at: https://beschermjegegevens.nl/en/.

Commissioned by the Centre for Investigative Journalism.

centre for
investigative
journalism

Epilogue

Gran knows why

AT THE DEATH OF MY GRANNY

My grandmother was born in 1920 and left school at the age of 12 to work in her father's shop. She has never used a computer (but has tried an iPod for audio books). At the age of 90, she is still interested in what I do.

Usually I just quickly skip over the technical aspects, because it is difficult for her to understand. The 'why' is much more relevant. Privacy, civil rights and the control of your own details/information. She understands this easily, without having to follow all the technical details of open source codes and cryptography.

Eben Moglen about digital freedom

In 2010 Bits of Freedom in Amsterdam organised a lecture and discussion with Prof. Eben Moglen, a former programmer who is now a law professor and advocate for the use of free software. Part of his lecture was about the risks of cloud computing (see a previous lecture[1] in New York on the same

[1] *https://www.youtube.com/watch?v=QOEMv0S8AcA*

theme). Besides his new plans for a technical project (the Freedom Box[2]), Moglen spoke mainly about the principles of digital freedom. Explaining this concept in The Netherlands remains difficult.

GENERAL, ITALIAN FORCES HAVE ENTERED EGYPT.
AS I EXPECTED. THIS IS A FOOLISH MOVE BY MUSSOLINI, BUT LIKE HITLER HE WILL NO DOUBT FORCE HIS COMMANDERS TO—
HEY. GODWIN'S LAW.
DAMMIT.
YOU KNOW, THIS MAY BECOME A PROBLEM.

A video[3] that Bits of Freedom tweeted about shows this problem. It is a short list of recent privacy breaches but does not explain why these are problematic. For many viewers there is still a pervasive feeling of "So what?".

In The Netherlands, the problem explaining this issue is that we have no recent experience of a government that has seriously gone off the rails (unlike Spain[4] and Eastern Europe). The use of a good recent example can be seen in an employee of the German T-Mobile explaining why the British government's Stasi-style tapping of all mobile phone traffic[5] might not be a good idea. Churchill must be turning in his grave.

[2] *https://wiki.debian.org/FreedomBox/*

[3] *https://www.youtube.com/watch?v=ZhXWN04c1Nc*

[4] *https://en.wikipedia.org/wiki/Francisco_Franco*

[5] *https://www.dailymail.co.uk/news/article-1238618/Telecom-firms-criticise-plan-Stasi-like-checks-phone-email.html*

History may repeat itself

As we have only experienced two real disasters in the Netherlands in the last 100 years (the German occupation and the 1953 flood), we as a people fall back on WW2 to explain the importance of civil rights. And then the Godwin-accusations fly.[6] For the post-baby boom generations the war is a (his)story that we read about, but which is not quite real. And the possibility that such a thing could happen again is inconceivable, and therefore unmentionable.

Wise grandparents

My grandmother has no such problem because she lived through it. A real war - where the previous government was suddenly replaced by a new administration that energetically started using data collected in previous decades, and which found the accurate ethnic records extremely useful: an administration, which could put your neighbours on a train to Westerbork concentration camp, and would shoot you for owning a radio.

Eben Moglen suggested that we all ask our grandparents why privacy and other civil rights are important. People who have lived through an oppressive state are largely immune to Godwin's rules. They can speak out from a personal, rather than an abstract, historical perspective. My grandmother is not well enough to speak out, but hopefully there are some grandparents out there who can explain to the younger, Facebooking and tweeting

[6] *https://en.wikipedia.org/wiki/Godwin's_law*

generation in the Netherlands the vital importance of privacy and other civil liberties.

When I'm done explaining things, Gran always grabs my hand and whispers:

"Just you be careful! Because you never know what could happen when you are criticising governments."

She knows this, so take a bit of time to listen to your gran.

Dedicated to my grandmother:
Tet de Boer-Olij, Kollum 1920 - Leidschendam 2010

Acknowledgements

Sponsoring:

- Beehive Techcampus 4.2

Proofreading:

- Floor De Backer

Cats (for allround support):

- Dita
- Mana

Image credits

Intro:

Old family photos - Family Kamphuis

Arjen sitting on the porch and on rock in Pakistan - Wim Korver en Wilma Tjalsma

Arjen holding baby - Photo by Ancilla van de Leest

Arjen on stage in Noordwijk - Photo by Marcel Verheggen

Part 1:

Chapter 1:

NSA strategic Partnerships - Leaked image from Snowden's stack, courtesy of NSA

Chapter 2:

Arjen behind desk - CC-BY Karola Riegler, 2017

Chapter 3:

Robohand holding a processor - iStockPhoto

Chapter 4:

Monkey with tool - Alamy stockphoto, Poster XS4ALL - XS4ALL, 2010

Chapter 5:

U heeft gestemd - http://wijvertrouwenstemcomputersniet.nl/, Cartoon - https://xkcd.com

Chapter 6:

Article 6.1: 1945 photo of a sailor kissing a nurse in Times Square on V-J Day.Iconic photo by Alfred Eisenstaedt. Found on Wikipedia: https://en.wikipedia.org/wiki/V-J_Day_in_Times_Square

Article 6.2: Printscreen

Article 6.3: Vintage W - Adobe Stock

Article 6.4: Lego pirate - Pixabay

Article 6.5: Pirate behind laptop - Pixabay

Article 6.6: No copyright sign - Pixabay

Article 6.7: Copyright symbol on YouTube - Pixabay

Article 6.8: HAR2009 logo - Used with permission, photos of HAR2009 discussion by Reinoud van Leeuwen

Article 6.9: Hamburg Parliament - Photographer unknown

Article 6.10: Copylock - Adobe Stock (also used on sargasso.nl)

Chapter 7:

Article 7.1: Europa riding a bull - Mosaic from the Bible around 3th c. AD, scenario text - source unknown

Article 7.2: Bluescreen image - Printscreen

Article 7.3: Milky Way - Source unknown

Article 7.4: Don’t tread on the Internet (meme on “Don’t tread on me”) - Artist unknown

Article 7.5: Asteroid hitting earth - Stock Reuters & UPI

Article 7.6: Flying raincloud - everystockphoto.com

Article 7.7: Asbestos - commons.wikipedia.org

Article 7.8: Flame - Pixabay

Article 7.9 & 7.10: X-ray - istockphoto.com

Article 7.12: Fingerprint of Minister Schäuble for the Interior of Germany - Print by ccc.de
Article 7.13: Chip Card public transport The Netherlands - Photographer unknown

Chapter 8:
Article 8.2: Eye - Pixabay
Article 8.3: Double thinker (meme on "The Thinker") - Artist unknown
Article 8.4: Summarian tablet - Free to use
Article 8.6: The Netherlands in Open Connection - Ministry of Economic Affairs of the Netherlands, € 7.800.000.000 image - Artist unknown (probably made by Arjen himself)
Article 8.8: Flag of Peru with Tux (Linux pengiun) as symbol - Artist unknown
Article 8.9: Arjen on stage - Photo by Yolanda, 2009 - Thanks to Yolande for taking the above image and making it available!
Article 8.10: Parrot in the Caribean & House on rock- Photos probably by Arjen himself
Article 8.11: #24C3 - 24th conference of https://events.ccc.de/

Chapter 9:
Article 9.2: Bookcover Pentagon Papers
Article 9.3: Wikileaks hourglass - Also on Stockphoto
Article 9.5: Dr. Strangelove - or how I learned to stop worrying and love the bomb - Stanley Kubrick - Stockphoto Alamy
Article 9.6: Pulitzer Prize - Originally by Daniel Chester French
Article 9.7: Mechnism - Stockphoto
Article 9.8: Philosoraptor (meme) - Basic picture in Stockphoto

Article 9.9: Troops - Pixabay

Article 9.11: PGP fingerprint - Probably from Arjen himself

Article 9.12: Cyberthief - iStockphoto

Article 9.13: Key - Pixabay

Part 2:

Before intro: Arjen sitting on wall in protective armour - Roger Renni, Director / Senior Security Advisor Reuters, 2018

Chapter 8: Cartoon - https://xkcd.com

Epilogue:

Cartoon - https://xkcd.com

Photo of grandma - Family Kamphuis

We live in challenging and confusing times for many following societal developments. Technology is rapidly changing our lives, society and the world. The times of blind and uninformed tech optimism are coming to an end. It's time to have a real conversation.

Arjen Kamphuis (1972) was a prolific speaker, writer and activist on the topics of digital rights, open source software, creative commons, privacy and mass surveillance. Inspired by his grandmother, he worked relentlessly to create awareness for a more free and democratic society, up until his mysterious and unresolved disappearance during a holiday in Bodø, Norway in August 2018.

Arjen's closest friends and associates have taken the initiative to catalogue the Dutchman's most thought-provoking and visionary words into this publication.

This book is for anyone invested in what the future will hold for humanity, and to be inspired on how to create a more safe, just and free world with the help of technological advancements.

Because Arjen's message is more important than ever.

ISBN 9789090328218
9 789090 328218