Ditch computers to save democracy: ethical hacker

March 3 2017, by Jo Biddle

(From left) PvdA Party leader Lodewijk Asscher, CDA Party leader Sybrand Buma and D66 Party leader Alexander Pechtold file in the 'Stemwijzer', an online voting guide for the Dutch elections, on March 2, 2017 in the Hague

In an age of superfast computers and interconnected everything, the only sure way to protect the integrity of election results is to return to paper and pen.

That is the view of Sijmen Ruwhof, an ethical or "white hat" hacker, who last month revealed that the Dutch election's commission computer software was riddled with vulnerabilities.

In a shock announcement just weeks before the March 15 elections—seen as a bellwether of the rise of far-right and populist parties across Europe—Dutch officials announced they were abandoning the computer system in use since 2009 to return to counting ballots by hand.

It was Ruwhof who discovered the problem. At the request of Dutch broadcaster RTL he spent just one evening examining the OSV software, developed for the Dutch government by a German company, via an online YouTube explanatory video, finding 25 weak points.

"It seemed to be completely insecure. I was quite shocked that we run our democracy, our election process based on very vulnerable software," he told AFP.

Within days of the RTL report, the interior ministry announced ballots cast by the 12.9 million eligible voters would now be hand counted.

Then the head of the Dutch secret services (AIVD) made another stunning revelation—in the past six months there had been hundreds of attempted cyber attacks on Dutch companies and government agencies. Most were believed to have been carried out by Russian, Chinese and Iranian hackers.

"It's a real challenge to stay ahead of the game," AIVD head Rob Bertholee said.

Weak spots

But these revelations, like the stunning news that Russian hackers appear to have meddled in the US presidential elections, were of little surprise to Ruwhof.

As a 12-year-old he became fascinated by computers. Self-taught, he managed to hack into the school computers and informed grateful teachers the system was insecure.

That was 19 years and an information technology degree ago. Now 31, Ruwhof makes his living working for banks, government departments, and major companies hacking at their request into their systems to expose their weaknesses.

"It's very easy," he insisted, without any smugness. But he remains frustrated that for many companies and organisations security is almost an afterthought.

In a shock announcement just weeks before the March 15 elections Dutch officials announced they were abandoning the computer system in use since 2009 to return to counting ballots by hand

"Software systems are so complex nowadays that it's hard for a single IT person to comprehend the whole system. So nobody has the total picture of the system. As a hacker you just go by and you scan for weak spots and you always find something."

The world has been lucky so far, because few terror groups like the so-called Islamic State have the capacity yet to unleash "cyber terrorism".

But imagine if from a computer far, far away malfeasants could snap the power grid, change the formula for purifying drinking water, or empty millions at once from bank accounts, undermining the financial system?

And that it is not the worst scenario.

"If you manage to manipulate election software, you can decide who runs a country, and that's a whole different impact," Ruwhof warned.

'Sophisticated spy devices'

His advice? "If you want to protect your system against state sponsored hacking, ditch your computer. You cannot trust it," he said.

Computers are "highly sophisticated spy devices" and they "are everywhere in our society"—with more and more devices from our cars to our coffee machines becoming interconnected.

Countries who want to use computers for vote counting should build

their own system from scratch. And they can't use existing operating systems for fear someone could have written a backdoor into millions of lines of code.

"You have to write your own operating system, you have to design your own hardware and you must understand that the election process is of the utmost high integrity. So you really have to have the highest standards for security," said Ruwhof.

But it's a hugely expensive prospect, and with time the software will degrade.

In the past elections "were always done without computers," Ruwhof said.

"Because there is a computer, we should use a computer? No, let's stick to paper. It's the most secure option."