Estonia: what doesn't kill you makes you stronger

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, Network Security

Lauri Almann didn't immediately understand what he was being told. He was at police headquarters watching a bank of TV screens depicting the destruction of the mediaeval quarter of his nation's capital. Live CCTV feeds showed rioters smashing windows and looting. A colleague entered the room to tell him the Government was having trouble posting press releases to its website. "Why are you bothering us with this?" asked Almann, his focus still on the violent images. "You don't understand, said the colleague, I think we're under cyber-attack."

This would certainly have worried Jaan Priisalu, if he'd been in a position to know about it. At the time, he was responsible for the IT systems of a major bank. But he had more immediate problems. After a pleasant day at the beach with his girlfriend he was trying to get back into the city. But there were police officers blocking the streets and helicopters overhead.

At that point, on 27 April 2007, neither man knew that they were facing three very grim weeks. The small but modern state of Estonia was suffering the world's first major cyber-attack on the infrastructure of an entire nation. At times, the assault would cripple the e-services on which the country had built a global reputation for innovation. But it survived, and in some ways may have benefited from the experience. So, in the intervening five years, what lessons have been learned? How does Estonia shape up today, in terms of cyber-security and its e-services? And what does it have to teach the rest of the world?

Ethnic tensions

In the many retellings of the Estonian story since 2007, the cyber-attacks are often portrayed as a spontaneous response to the politically inflammatory treatment of a statue. In fact, they need to be put within a broader perspective of political and cultural tensions with roots going back into history.

Estonia is both a very young and a very old country. Somehow it has maintained a unique cultural identity in spite of having spent the majority of its existence under foreign occupation or control. There was a brief burgeoning of independence after World War One, before the nation was once more 'liberated', this time by the Soviets. In fact, they didn't so much liberate it as simply occupy territory vacated by the fleeing Nazi forces – a distinction underlying the tensions that ultimately resulted in the 2007 riots and cyber-attacks.

Estonia finally gained full independence in 1991, following the collapse of the Soviet Union and the country's peaceful 'Singing Revolution' of 1989. It wasted no time in re-inventing itself as a modern, networked nation. It skipped several stages of technological evolution, embracing e-services such as online banking with an enthusiasm and an adoption rate that many Western European nations could only envy. And it prospered: the Internet society supported a healthy economy.

But no nation is without its problems. Around a quarter of Estonia's population does not consider itself Estonian. They are generally classed as 'Russian', as although in terms of ethnicity they originate from a number of countries, most speak Russian as a first language. A hard core of them believe they are treated by the state as second-class citizens.

These tensions translated into protests, often centered around a memorial in the centre of Tallinn. This statue of a Russian soldier was one of many erected across Europe by the Soviets commemorating their war dead. But just as some of Estonia's Russian population viewed the monument as a symbol of their strong cultural links to Estonia's eastern neighbour, so some Estonian nationalists viewed it as an affront to their independence, because they saw the Soviets not as liberators but as invaders. What was a reminder of wartime sacrifices to some was a symbol of decades of occupation and oppression to others.

On 9 May 2006, protestors from opposing camps confronted each other around the edifice. There was no violence but the potential was clearly there. This prompted a debate in Government, culminating in a decision, declared nearly a year later, to move the statue – and the Soviet soldiers buried beneath it – out of the town centre to a military cemetery. This move was planned to be completed by 9 May 2007, the date being announced in advance. But work on the site actually began on 26 April, which prompted a demonstration – peaceful at first but which soon descended into rioting – the so-called 'Bronze Night'.[1]

It was this violence that Almann was watching on the CCTV monitors. At the time, he was Permanent Under-Secretary of State for the Estonian Ministry of Defence and a member

of the Government Crisis Committee (similar to the UK's Cobra disaster management committee).

Network Security interviewed Almann on the occasion of the Fourth International Conference on Cyber Conflict (CyCon), held in early June 2012 in Tallinn under the auspices of NATO's Co-operative Cyber Defence Centre of Excellence (CCD COE), also located in Estonia's capital.[2,3]

"Tallinn is not used to riots," says Almann. "We've had the First World War, the Second World War and the football game with England – that's it." He adds, more seriously: "It was a sight that we had never witnessed. People smashing in windows, going in jewellery stores and fashion shops and simply looting. And we thought, 'this is the crisis'."

In the early hours of the following morning the authorities moved the statue to a secret location (it was re-erected in the military cemetery and rededicated on 8 May). But as Almann and the Government were about to find out, the riots would soon abate to leave them with a more serious problem. The cyber-attacks started that evening, 27 April.

At first sight, the cyber-attacks might appear to have been a spontaneous reaction, much in the same way that some people were prompted to smash windows. But closer examination shows that the most effective assaults were carefully organised and almost certainly pre-planned.

Anatomy of the attacks

The first attacks consisted of denial of service floods – some using junk mail – against high-profile websites, most of them with connections to the Government. They included websites for the President, Parliament, police and political parties. The 'public briefing room', where the Estonian Government posts its press releases, was among the first hit and was soon inaccessible from outside of the country. There were also a number of site defacements.

Much of this was co-ordinated by Russian hackers using online forums. Using a methodology that would later be adopted by hacktivist groups such as Anonymous, the hackers encouraged 'patriots' – many without technical skills but sharing a desire to take action – to download ready-made software. These were mostly pre-existing DDoS tools that employed ping or SYN flooding, but some had been specially modified to participate in the attack on Estonia.

Figure 1: The Soviet-built memorial to Russian Second World War dead that became the focus of political protests – shown at its new location at a military cemetery. Source: Hannu/Wikipedia.

Media outlets, including the daily newspaper *Postimees*, also came under attack and at one point the media found itself cut off from the outside world. This, Almann reckons, is indicative of how well planned the attacks were. "It was disturbing," he says. "It was already difficult to read news inside, but it was also difficult to read news for those people who were outside of the country. There was a panicky feeling starting to grow. That was the moment also that the journalists started to ask inconvenient questions – 'what about this great Estonian e-government?' and 'what are you going to do about our newspaper being under attack?'. I think that was the major wake-up call for the newspapers. Because nobody cares if you cannot access the President's website, let's be honest."

The attackers also turned their attention on the websites of town councils and schools in outlying regions of the country. Parliament was denied the use of its email system for 12 hours. And on 1 May, a number of Estonian ISPs had to cut off their customers for 20 seconds to reboot their systems.

DDoS attacks are hardly rare. So what was the first clue that this was something out of the ordinary? Almann says that the Computer Emergency Response Team, Eesti (CERT-EE), based at the Centre for Information Technology (Riigi Infosüsteemi Amet, RIA), almost certainly knew very quickly just from the scale of the attack.[4] For him, it was the political nature of the targets: "Simply the fact that the Government was unable to release its press releases when it wanted in the middle of a crisis is pretty bad," he says. "Now that we know more about it, the attack was not significant, not sophisticated [from a technical perspective]. I think what was significant about it and why it reached such high levels of government was that it coincided with political attention. It was solely politically motivated."

Fighting back

Within 24 hours of the attack beginning, so had the fight-back, with a co-ordinated effort based at the Ministry of Defence and working in co-operation with CERT-EE. Right away, work began on identifying attack signatures to allow filtering of malicious traffic. This effort was supported by co-ordination between CERT-EE and other CERTs around Europe.

While most of the attack traffic originated from abroad, some of it was domestic. The police soon made an arrest and a suspect was shown on TV – an act that some sources credit with a

'deterrent effect'. By and large, though, the first week of the attacks was pretty chaotic, on both sides.

On 4 May, a second wave started, more organised this time, and botnets started to make their presence felt. There was a slight drop-off during the period 6-8 May, but it was the calm before the storm.

Russians celebrate victory in World War Two on 9 May, which is why ethnic Russian Estonians had gathered at the memorial on that date the previous year. The botnets that swung into action that day were now much bigger: as a rough estimate, as many as one million computers may have participated in the main attack, and some calculations put the total number of machines involved over the whole campaign at two million.

"The idea was to have a huge gathering on 9 May that was combined with a huge cyber-attack," says Almann. "The main botnet was rented for that purpose."

It's probable that the attackers always intended to launch their campaign on this date, but were spurred into premature action on 27 April by work beginning on moving the statue. This delay in the main assault turned out to be a big mistake. According to Almann, the size of the attack that was mounted on 9 May was two to three times the Internet capacity that Estonia had in place before the troubles began. It would have completely overwhelmed the country. But the earlier, less concerted attacks had prompted the authorities to deploy countermeasures (such as filtering) and also increase bandwidth. So the new assault failed to shut down the Internet in Estonia entirely.

It was still serious, though. Banks were targeted now, particularly Hanspank and SEB Eesti Uhisbank. For short periods of time over the coming week they were prevented from conducting Internet business or making transactions abroad. For Almann, that was another ratcheting up of the seriousness. "If you don't get access to the President, that's one thing; if you can't get access to the media, that's another; but if you can't get access to your money, that's going to be a problem."

Professionalism

The attacks lasted, in one form or another, until 18 May. At their peak, traffic flows hit 1Gbps. By today's standards, that's not huge – some businesses today greatly exceed that in their daily operations. But even though it is such a 'wired' country, in 2007 that level came close to exceeding Estonia's bandwidth. Arbor Networks, which monitored and reported on the campaign, said that it detected 128 unique DDoS attacks on Estonian websites. Most lasted less than an hour and generated no more than 30Mbps of traffic. A quarter of the attacks were bigger than this and the top 10 ran at 90Mbps and lasted as long as 10 hours.

Priisalu, who is now director general of RIA, says that he saw 82,000 botnet-controlled computers targeted at the bank he was working for at the time. He reckons the botnet must have been prepared well in advance. "And this thing was professional, too," he adds, "because it contained intelligence and it was saving energy." Most botnet-based DDoS attacks, used for purposes such as revenge (their most common usage in Estonia), are fairly dumb, simply throwing as much traffic as possible at the target. But not this time. "If you were successful in filtering them out, if you were not responding anymore, they were actually throttling their attack rate," he explains. "So it's clear they were tuned in a sense. Amateurs do not conserve energy, professionals do."

Further evidence came when the bank decided to measure the size of the attack against it. That meant taking down its defences. "At one time, we removed all the filters for one minute, and in 10 seconds the pipe was full," he says. That means the botnet system contained built-in intelligence to use its available bandwidth effectively. "Humans cannot react to the configuration change so quickly," he points out.

Attribution is difficult

So who, precisely, were the attackers? This isn't as simple a question as it seems. It's a truism of cyberwar that

Early warnings

The Estonian attack is often portrayed as a kind of digital 9/11, occurring out of the blue with maximum surprise. In fact, an attack was expected, and some preparations had been made.

"We had warnings from the intelligence services," says Almann. "Not about this attack – but since we were so e-services based, we were probably going to be attacked."
In fact, Almann said as much in a newspaper interview in Dec 2006. "The Government's reaction was to co-operate with private sector companies. A Memorandum of Understanding (MOU) was signed with each of a number of 'critical' firms – banks, telecoms and so on – and an information exchange process was set up that also involved RIA and the Ministry of Defence.

A close watch was also kept on certain online forums where plans were being developed to attack Estonia.

The intelligence services believed the attack would come at the time of national elections, in March 2007. They were the first government elections in which citizens could vote online. (Today, around a quarter of Estonians choose to vote this way.) So sure were people that certain factions would take the opportunity to disrupt the elections digitally that the Government carried out a cyber-defence exercise.

In the end, the elections passed off smoothly, but Almann believes the exercise helped put people at the senior levels of government in the right mindset – that something could happen at any time – and helped to open channels between departments and other actors who would need to exchange information when a real attack came. Estonia being a small country, some of these connections – including those between the private and public sectors – were made informally, and turned out to be highly valuable.

attribution is difficult. All the same, and without engaging in Internet forensics, one can see the hand of the Russian state in at least some of the activities targeting Estonia. The cyber-attacks did not take place in a vacuum. Over roughly the same period of time, crossing the border from Estonia into Russia suddenly became very difficult. Rail lines were put out of action by unscheduled 'repairs'; bureaucracy at border crossings became a nightmare; and Russian organisations cancelled orders with Estonian firms.

In concert with the cyber-attacks, the pro-Putin Nasji movement in Russia organised a blockade of the Estonian Embassy in Moscow – something the city's authorities did nothing to stop. One Nasji leader even claimed responsibility for the cyber-attacks, saying they were launched from the Transdniester region of Moldavia and that the Russian administration was not involved. It's notable, also, that the peak of the attack, due to start on 9 May, actually began at 23:00, 8 May in Estonian time. That happened to be 00:00, 9 May in Moscow time.

So it is easy to blame the Russians. But actually, it is too easy. Among the mistakes that Almann admits to was a claim of direct involvement by the Kremlin. "There were some ping attacks that came from Kremlin IP addresses," he says. "Some guys in the Kremlin PR department were just trying to … partake." Somebody in an Estonian government department decided to present these IP addresses to the international media as proof that the Kremlin had organised the attacks, which required some backtracking later.

Nevertheless, Almann is still in no doubt who was behind the attacks, even if they didn't get their hands dirty. "Silence speaks more than a million words when it comes to attribution," he says. "In cyber-attacks, when we talk about attribution, we shouldn't focus on technical aspects and IP addresses. Estonia was attacked by a million to two million bots located in 175 jurisdictions. Roughly all – 174 jurisdictions – co-operated with Estonia in taking down the bots. There was one jurisdiction of one country which did not co-operate. So what does that tell you about the attribution? When it comes to cyber-attacks like that, failure to co-operate, failure to exchange information, should equal attribution."

Of course, Russia is notorious for not co-operating in areas such as cybercrime investigations. But Almann refers to customary international law and cites (with some pride) 'Martens Clause'.[5] Fyodor Fyodorovich Martens was the Estonian-born Russian delegate at the Hague Peace Conferences in 1899 and a declaration made by him was included in the preamble to the Hague Convention II – Laws and Customs of War on Land. In essence it says that if current laws cannot cope with novel situations – such as technologies that were not foreseen – then common sense should prevail.

"This is the Estonian contribution to international law," says Almann. "And it applies directly, I think, in cyber-warfare. We should use our common sense. And when it comes to attribution, if there's a country that doesn't co-operate while everyone else is co-operating, in an international large-scale incident, then that should make the attack automatically attribute to that country."

Need for co-operation

It didn't take long for people to start drawing conclusions from the whole experience. A paper in the Estonian Foreign Policy Yearbook 2008 says: "The main lesson lies in the fact that asymmetry of threats in the Internet era requires new and different approaches in addressing risks in society. The Estonian reaction to the attacks was rapid and professional, facilitated by an informal small network of Internet security community, which assembled immediately for a co-ordinated response. Secondly, the major practical lesson, regarding the future handling of similar attacks, would be an improvement of the crises management procedures and critical infrastructure protection plans, with a special focus on regular compulsory tests and simulations."[6]

Close relationship

There is a certain irony in the fact that Estonia and Russia actually enjoy extremely good formal agreements for law enforcement co-operation. These were signed in 1992 during what Lauri Almann, ex-Under Secretary of State for the Estonian Ministry of Defence, describes as "a very short window when relations were excellent". Very few countries have this sort of arrangement, he says. For example, "local police in any Estonian city can directly contact local police in any Russian city for any proceeding that they are undertaking. It's very rare, it's very strong and it's very effective in drug trafficking, people trafficking – and it's working right now. We are using this daily."

Invoking this agreement during the attacks, the Estonian General Prosecutor contacted his Russian counterpart asking for information on certain IP addresses and to talk to the people associated with them.

"The letter came back from Russia saying: 'We do not co-operate because our criminal code does not recognise the procedure identification of IP addresses'," says Almann. "We sent another letter saying: 'Why don't you check again?' And the letter came back: 'No, we cannot do anything because this is not a procedure. In our criminal proceedings, Russian police do not identify IP addresses' – which is a joke. Looking back, I think that maybe we should have written a third letter, and a fifth letter and a hundredth letter, and just kept hammering them. We didn't. We just quit and said, this is enough lack of co-operation."

Co-operation is the key here – and Estonia didn't get all the help it needed during the attack. For example, government departments sought web hosting services in other countries in order to get their sites up and running again. According to Almann, one EU country, which he wouldn't name, said something to the effect of, 'no, we don't

want to have anything to do with it, because we may come under attack'.

"Of course, this later raised all kinds of questions," he says. "What are the obligations of EU countries? What are the obligations of NATO countries in those events? Those same questions came up very politically afterwards, when the Georgians were under attack [the following year]. It is still an issue. It is still not solved."

Cross-border co-operation was then, and to a large extent still is, hopeless. Almann, who has now gone back to his profession as a lawyer, still involves himself with the issues. He's involved with an NGO called the European Cyber-Security Initiative that runs exercises focusing on the decision-making and legal aspects of cyber-defence, and helped to organise the Tallinn CIIP exercise, which focuses on the senior government level.[7]

The decision-making challenges are crucial, but it's also important that it's all pitched at the right level. "A dangerous trend I see – or saw, at least, at some points – when cyber-awareness starts to grow, was that all the countries were suddenly focused on who was the cyber-tsar. A cyber-tsar is important, and I agree that we should have a high level of co-ordination and awareness in high levels of government. But I think the key to effective response is not how high we develop it, but how low is the effective co-operation. It has to be at the operational level. And in certain cases it has to be artificial intelligence that is co-operating, because human beings are unable to respond in certain cases – because of the need to respond so fast."

At CyCon, Steve Purser, head of the Technical Competence Department at the European Network and Information Security Agency (ENISA), also strongly emphasised the co-operation issue.[8] "There's no agreed structure for cross-border security," he said. "We need to improve processes for information sharing. We need cross-border response mechanisms. And security technology needs to be able to operate in a cross-border environment."

But he also acknowledged that every country's cyber-resilience is shaped by national concerns and goals, that there is no governance structure that would support the processes required to develop this kind of international co-operation and that private-public co-ordination even within a single state is difficult to achieve – a thorny issue when so much of the critical infrastructure is in private hands.

There's also the issue of whether you tell people about the attacks. Private organisations face new disclosure rules that will force them to come clean about data breaches. But at the national level, much is still clouded in state secrecy.

During the Estonian attacks, not everyone in the Government was convinced they should tell the world about it. "There was actually a debate, and some of the people inside were arguing that we should have a very low profile because it might be damaging to our e-government reputation, that we should downplay it, say that DDoS is not important," says Almann. "And then there were those people who prevailed, who said that we should go public, say 'this is a threat', 'this is a cyber-attack and the country and the world needs to know what's going on'. And I'm very glad it turned out this way and I think we made the right decision."

Could have been worse

Perhaps the most compelling lesson of the 2007 attacks it that it could all have been so much worse. Almann insists that the country actually sustained no long-term damage, although there were serious immediate costs incurred through lost productivity, lost business and the cost of remediation – not least because the backup hosting they did eventually obtain was often at triple and quadruple the normal rates.

Aside from the expenses incurred by banks and other private organisations, it's also worth noting that there is no publicly released data about attacks on other forms of critical infrastructure – such as SCADA systems managing the electricity network. That's not to say there weren't any, just that the data isn't available if there were. It's possible that some details remain sensitive and classified. In that sense, then, it's difficult to judge precisely how close the country came to collapse. What's more, in the heat of the conflict, not everything was being logged.

Yet even if all the data were readily available, enumerating the potential for damage is no easy job. There are steps being made in this direction, however. At CyCon, Assaf Keren, product manager, cyber security for Israel-based security firm Verint, presented the Cyber Attack Susceptibiity (CAS) index.[9] "We wondered whether you can measure whether the Internet is a critical infrastructure for a country," he told the CyCon audience. CAS combines two key indicators – the UN's e-Government Development Index, which measures to what degree a nation's government has put its activities online, and an Internet usage percentage, which assesses how much citizens use, and therefore probably rely on, online services.

Had this been around in 2007, one might have expected Estonia to rank highly on such a scale. And it's not as though the CAS index is addressing new forms of cyberwar. In his presentation, Keren cited the cyber-attacks undertaken by both sides during the 2008/9 Gaza War (called Operation Cast Lead by the Israelis). DDoS and massive website defacements were the key weapons in the cyber components of this battle, and there were some damaging effects. Keren characterised as "psychological warfare" the defacement of a hospital website with pictures of wounded Israeli soldiers. Yet even with the CAS, which Keren says is a work in progress, it's difficult to judge to what extent the Internet can be classed as critical infrastructure.

"It's murky," Keren told *Network Security* after his presentation. "It's not as clear-cut as electricity and water. If you take down power, people die. This is more about the fabric of life. Although that can involve loss of life." One of the sites that went down during the Cast Lead conflict, he says, was one providing key, life-saving safety information – for example, what to do in the event of attacks such as rocket strikes. Yet more work needs to be done to differentiate

between inconvenience and real damage and Keren thinks this should be possible.

"I think what I'm saying here is that, the higher you get on the [CAS] index, the Internet probably is critical infrastructure," he says. "If Israel loses the Internet, then it's going to harm more than just the convenience of the citizen. It's going to harm the military operations, it's going to harm the banks, it's going to harm hospitals and a lot of things that are critical infrastructure. That's the basic premise of the research."

Bad rep or good advertising?

Any organisation will tell you that one of the most threatening aspects of a DDoS attack is the damage it can do to the corporate reputation. And Estonia has built the whole country's international reputation on high technology. But Almann thinks the long-term result has been positive.

"The decision not to downplay the attack and be honest about it, and actually to use the attack as a showcase of the wider problem that we have was the right one," he says. "Ironically, I think that Estonia has gained in e-reputation. And there are some strange consequences to that."

He points out that the majority of people assume that the NATO CCD COE facility was located in Tallinn as a response to the attacks. In fact, Estonia started work on the proposal for the centre in 2003 and started lobbying for it in 2004.

The centre was opened in 2008. It provides training courses and conferences, such as CyCon, focusing on strategic, legal and technical issues. In late 2012, it will publish 'The Tallinn Manual' on international law applicable to cyber warfare. And it hosts collaborative exercises: in March 2012, for example, it held Locked Shields which simulated telecoms companies coming under attack.[10]

It's an accepted truth that most commercial organisations don't appreciate the value of security until they're been attacked. And that translates to the national level too. Before the Estonian attacks, the CCD COE was, says Almann, "hugely unpopular in NATO because everybody thought it was a non-issue. And we had only one member in the NATO centre at that time. Then we had some other countries that started to co-operate before the attacks. But after the attacks, everyone understood that this is a right thing, a good thing to do, and the NATO centre gained in membership."

Figure 2: Participants in the Locked Shield exercise, held at the NATO Co-operative Cyber Defence Centre of Excellence (CCD COE) in Tallinn.

Another positive outcome was that the incident proved the robustness of Skype, which was born in Estonia and is still developed and maintained there. Thanks to its peer-to-peer design, it came through the whole thing unscathed.

Almann characterises the whole Estonian IT community as having been "extremely disciplined" during the attacks – not least for refraining from mounting counter-attacks. That discipline inspired the creation of the Cyber Defence League which operates under the umbrella of the Kaitseliit (Estonian Defence League – similar to the US National Guard). It consists of IT specialists who train together on cyber-defence.

Almann believes the positives outweigh the damage that was caused. And possibly the biggest benefit has been awareness. "I think one of the most important things is the worldwide knowledge and the attention that the world started to pay to this," he says, pointing out that NATO's cyber-security strategy and the EU's investment in cyber-security directly followed the attacks.

Not that Almann is recommending getting attacked as a path to enlightenment. "It didn't look like this big success story in the second week of the attacks, let me tell you," he says. His biggest fear at the time was the unknown. There were concerns that, under the cover of the DDoS assaults, the attackers might be carrying out more damaging cyberwar or cyber-espionage activities (as was seen in Georgia the following year). And there was no knowing when it would end. It wasn't like a conventional battle in which the victors prevail through skill, technology or overwhelming force. "The cyber-attacks didn't end because we were particularly good, or we came up with a magical solution," he says. "They ended because whoever was perpetrating these attacks decided to end it."

Estonia today

So what does Estonia look like today? The answer is, more wired than ever. The attacks failed to dent the citizens' confidence in the e-revolution that has brought so much wealth and convenience. Thanks in part to having started with a clean slate – the years of Soviet rule left the country with very little in the way of infrastructure – and because it's a small country (population

around 1.4 million), Estonia has built a highly integrated set of e-government services that has extended out to the commercial sector in areas such as banking.

Much of this is built around what is usually referred to as an ID card, although that's a term that the Government is trying to replace. The card carries a chip with two digital signatures linked to the individual's identity number, which is assigned at birth. Citizen's just need to remember two PINs – a four-digit one for logging on to online services, and a five-digit one for signing. While the standard card carries a photo and other ID information, citizens can opt for a non-photo alternative, or for a special SIM to use in their mobile phones.

Signing is used for everything from online purchasing and e-banking through to signing legal documents online and voting. (Citizens can vote as often as they like in any election, but only the last vote counts. One old woman apparently voted 500 times in the last election because she enjoyed it so much. Perhaps she remembered the Soviet days.) Digital signatures carry the same legal weight as physical ones. The signing is carried out using the embedded keys in the card and confirmed with the PIN. Citizens place their cards into a card reader: with the mobile phone version, out-of-band tokens are used. The phone version works over the mobile network – no Internet connection is needed.

The result is that 99% of banking transactions and 94% of tax declarations are made online. It helps that all schools and government offices have broadband, and more than 1,100 public wifi access points mean that connectivity is available pretty much everywhere, including some national parks. More than two-thirds of homes have broadband. And although such a small country, Estonia has four 3G and two 4G networks.

Unified infrastructure

Supporting all of this is an IT infrastructure of unusual coherence. While data about a given citizen might be spread across multiple databases in both the private and public sectors, each individual item of information is generally stored in only one place. The databases – in government departments, insurance, banking and telecoms companies, and so on – are linked by a middleware backbone known as the X-Road. This has provided a common data interchange format allowing the extensive integration of all kinds of services.

Each system can pull information from the other databases, although strict data classification and access rules determine who can see what. Citizens also have the ability to see – online and at any time – who has been viewing their data because the person's ID number is always logged. If they think the access is inappropriate, they can complain to the Data Protection Agency. The person who accessed the information then has seven days in which to justify the access.

Getting the private sector to engage with this infrastructure wasn't too difficult – they had commercial reasons for getting on board, and banks were among the first to sign up. In part, this is because the system provides firms with a ready-made authentication framework.

A Nordic Silicon Valley

Estonia's love affair with technology pervades the business sector, and the country is keen to position itself as a kind of Silicon Valley of Eastern Europe. Around 60-70% of start-ups are IT-related firms.

Aside from Skype, which was founded in Estonia, a large number of high-tech firms have made it their base. They include foreign-based firms such as GuardTime (Singapore), Biometry (Switzerland) and ICD (Norway) which have based R&D operations in Estonia. And there are many home-grown firms, such as TV and radio network operator Levira in which the state owns a 51% stake.

"A good example of public-private partnership is that the authentication for the [ID] card is done by a private company," explains Luukas Ilves, who is responsible for international co-operation at RIA. "So they had a financial and economic incentive to maximise the use of their service. They got a trivial amount of money for every digital signature, for every authentication. But then the banks that use it and the government agencies that use it for authentication, they pay for this. It's a small amount of money, and they save huge amounts because they don't have to do their own infrastructure for authentication, either digital or paper. So you have a company that has an economic incentive to push the adoption, and then wants to negotiate the deals, wants to find more customers. You can't do it just as a public good because often then you'll actually lack the incentives that will make this work across the market economy."

"Taking down the core servers of X-Road doesn't kill X-Road"

Citizens were a different proposition. "Educating the users is the most expensive thing," says Priisalu, adding that Estonia's year-zero approach, in which it started from very little in the way of technology penetration among the population, certainly helped because, "behaviours were not written in stone."

Estonia started with a major effort to teach people how to use the Internet – which included security awareness. Then, in 2005-2009, there was a major education campaign around e-services.

Target-rich environment

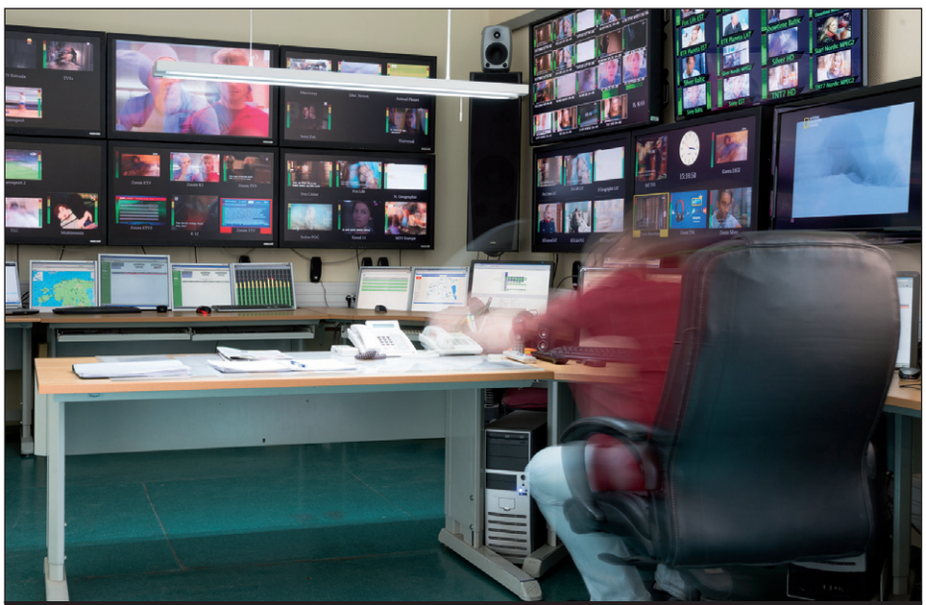
What all this adds up to is a nation even more dependent on its information infrastructure than it was during the attacks of 2007. For example, given that data is often held in one database and then shared across systems via X-Road, it would suggest that an attack on a single target might cause widespread disruption.

"The first thing is that it's distributed, through the X-Road middleware layer," explains Priisalu. "Taking down the core servers of X-Road doesn't kill X-Road." But, he adds: "There are choke points and critical points, and it's quite clear that you can degrade the government operation. So if you're asking whether it's possible to attack society with cyber-attacks – yes, it's possible." But, he points out, that degradation will only go so far before the crisis management processes that have been put in place kick into operation. And the integrated and co-operative nature of Estonia's IT infrastructure means that response can be very effective.

It's clear, even without reference to the framework developed by Verint's Keren, that the Internet would have to be considered critical information infrastructure in Estonia. So who defends it?

The answer is the same as anywhere else – each organisation, public or private, is responsible for its own piece of the picture. In many countries, this has created some highly problematic tensions. In the US, for example, a visceral dislike of government poking its nose into the operations of private firms, or dictating to them how they should go about their business, means that the Government has very little control over how certain elements of critical infrastructure – the electricity network, say, or railways – are protected. There is limited co-ordination, very little oversight and no coherent strategy. And even when a government might be able to dictate how a firm protects its infrastructure in the national interest, there's the thorny issue of who pays for that.

Almann cites a precedent, in the shape of the 2006 EU Data Retention Directive. Many companies complained bitterly about being forced to shoulder the burden this imposed. In Estonia, they took a simple approach: where firms incurred expense from this government-imposed requirement, the Government paid. "But we are a small country and we can afford it," admits Almann.



Estonia is now home to a large number of high-tech companies such as TV and radio broadcast network operator Levira.

And even so, the cost of protecting critical information infrastructure is still borne by the companies themselves. This is an issue in Estonia, as elsewhere, because so much of it is foreign-based. Most of the banks are Swedish or Danish; the biggest shareholder in the national energy company, Eesti Gaas, is Russian gas giant Gazprom; the oil companies are the major multinationals.

The national Critical Information Infrastructure Protection (CIIP) plan obliges companies to create and maintain contingency arrangements to ensure continuous operation. And they bear the cost of this themselves.

"This is part of being the dominant player in the market," explains Priisalu. "If you are a small company, then you are not part of this. People are not depending on you critically. But if you expand your business and take the dominant role, and you create a dependency on you, this also creates an expectation."

In a sense, then, the cost of protecting your infrastructure is the price of success.

Not everything is in place, though. The Government is still going through a process of defining security requirements. For the most part, this is not defined in terms of technology or capabilities, but what Priisalu defines as "process goals". The aim is to get firms to ensure a level of service even when under attack.

So how do the requirements for assisting national security fit with organisations' intrinsic security needs, which they would have addressed anyway?

"Actually, it aligns quite well," says Priisalu, although it depends on what view you take. "I would say it does go very well with the long-term business

goals. But in the short term, it might create planning problems for people. But this is nothing new, I think."

Given that many of the CIIP goals are still being defined, how secure does Priisalu feel right now? "We know what the levels of dependence are," he says. "We have done two audits of the majority of the critical information providers. So we know roughly what the dependability level is. We have some scenarios we have played through together and it's quite clear there is still lot of work ahead. But we have very good co-operation with the technicians, and what we're doing right now is making the management guys understand why we're talking about this."

And given the emphasis that so many are placing on international co-operation, to what extent is this readiness confined to Estonia and to what extent does it involve co-operation with other countries? "I wouldn't say that there is much that has been done here," he says. But he also points out that companies don't create their systems according to some national plan – they do it for themselves. And given the international nature of many of these firms, and the business they conduct, a large number of the systems in private hands are already built on multinational infrastructures.

Conclusion

The attack on Estonia provides an object lesson that what doesn't kill you makes you stronger. It focused minds and efforts and highlighted how defending a nation against cyber-assault is not a matter of technology but of political and operational co-operation. Whether the will and the resources exist to realise that co-operative infrastructure across Europe and perhaps beyond remains to be seen. It's still a work in progress and, in the meantime, we become ever-more dependent on information infrastructures.

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is editor of Network Security *and its sister publication,* Computer Fraud & Security *and a Certified Ethical Hacker. He is also author of the novel* Black Project*, published by WebVivant Press (www.webvivantpress.com).*

Resources

- 'Large scale Internet attacks'. Swedish Emergency Management Agency (SEMA), 2008. This contains an excellent blow-by-blow account of the Estonian attacks before going on to analyse what the implications are for national security. Accessed Jun 2012. https://www.msb.se/RibData/Filer/pdf/26164.pdf.

References

1. 'Bronze Night'. Wikipedia. Accessed Jun 2012. http://en.wikipedia.org/wiki/Bronze_Night.
2. CyCon – International Conference on Cyber Conflict. http://ccdcoe.org/cycon/.
3. NATO Co-operative Cyber Defence Centre of Excellence (CCD COE). www.ccdcoe.org/.
4. RIA. www.ria.ee/en/.
5. 'Martens Clause'. Wikipedia. Accessed Jun 2012. http://en.wikipedia.org/wiki/Martens_Clause.
6. Tiirmaa-Klaar, Heli. 'The emerging cyber security agenda: threats, challenges and responses'. In 'The Estonian Foreign Policy Yearbook 2008' edited by Andres Kasekamp. The Estonian Foreign Policy Institute, Tallinn, 2008. ISSN 1736-4175. www.evi.ee.
7. Tallinn CIIP Conference. Accessed Jun 2012. www.riso.ee/tallinnciip/?id=main.
8. ENISA. Accessed Jun 2012. www.enisa.europa.eu/.
9. Keren, Assaf; Elazari, Keren. 'Internet as a CII – a framework to measure awareness in the cyber sphere'. In proceedings, 4th International Conference on Cyber Conflict, IEEE, CCDCOE, pp.111-123.
10. 'Locked Shields'. NATO CCD COE. Accessed Jun 2012. www.ccdcoe.org/334.html.

EVENTS CALENDAR

16–17 August 2012
Security B-Sides Los Angeles
Los Angeles, California, US
www.securitybsides.com

17–19 August 2012
SecurIT 1st International Security Conference on Internet of Things
Kerala, India
www.securit.ws

20-24 August 2012
The Fourth International Workshop on Organisational Security Aspects (OSA 2012)
Prague, Czech Republic
http://bit.ly/LLiBHO

20–24 August 2012
ARES – The 7th International Conference on Availability, Reliability and Security
Prague, Czech Republic
www.ares-conference.eu/conf/

30 August–2 September 2012
44Con
London, UK
www.44con.com/

10–13 September 2012
(ISC)^2 Security Congress
Philadelphia, US
www.isc2.org/CommunityPage.aspx?id=7927

16–24 September 2012
SANS Network Security 2012
Las Vegas, Nevada, US
www.sans.org/info/105035

21 September 2012
Security B-Sides St John's
St John's Newfoundland and Labrador
www.securitybsides.com

26–27 September 2012
Brucon
Ghent, Belgium
brucon.org