2020

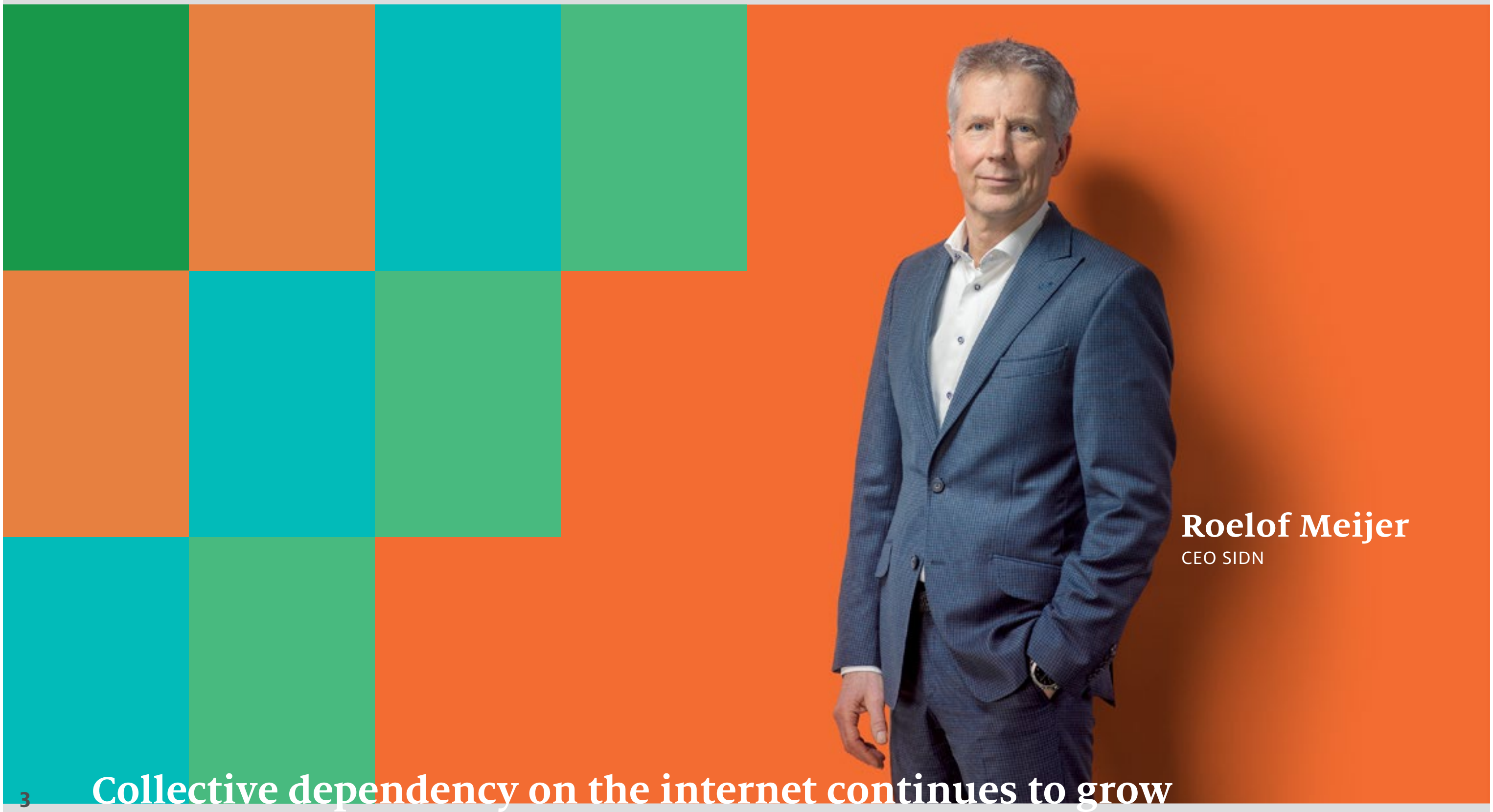
Annual Report

SIDN For confidence online

2020

Content

Foreword


Roelof Meijer
CEO SIDN

Collective dependency on the internet continues to grow

Learning from a crisis

An overstretched healthcare system; lockdowns, curfews and quarantines; closed schools and the complete shutdown of various industries. Thousands of deaths in the Netherlands alone, and millions worldwide. Economies everywhere plunged into crisis. 2020 was a year we certainly won't forget, and hopefully won't experience the like of again. And, despite rapid testing and vaccines, many of 2020's ills remained with us at the dawn of 2021.

However, just imagine what it would have been like if the pandemic had happened twenty years ago, when the internet was young. The consequences would have been disastrous. As it was, the internet enabled many people to continue working from home and kept large parts of our economy and society running. We were also able to keep in touch with our families and friends online. And, while things were generally hard for the business community, some entrepreneurs saw – and took – new opportunities.

As well as being the year of the pandemic, 2020 will go down in history as the year of hyper-digitisation. Many businesses 'went online'. The number of webshops soared. Everyone was ordering on line, arranging collections and getting things delivered. For popular webshops and delivery services, it was a golden period. New business models emerged, from starred restaurants offering takeaways to fitness centres providing remote coaching by webcam. Schools developed online teaching methods, concerts and symposiums were streamed and museums gave virtual tours. And, while some such services are merely stopgaps that will inevitably disappear when society reopens, others have real promise and will hopefully continue when the pandemic is over.

> *While things were hard for the business community, some entrepreneurs saw – and took – new opportunities.*

As a consequence of society's dash for the internet, we reached the milestone of six million registered .nl domain names on 18 June, more than six months sooner than forecast. The name that took us past that marker was deyogiclub.nl, registered by a yoga coach in Neede: a classic example of an entrepreneur spotting an opportunity amidst the crisis.

Smooth transition

Our organisation too was significantly affected by the coronavirus crisis. However, we quickly adapted to everyone working from home, and the transition went smoothly. Already having a strong commitment to ensuring service continuity under all circumstances meant that we were well prepared for working away from our usual desks.

We helped staff to set up proper home workstations and placed a lot of emphasis on internal communication and teamwork. As a result, we were able to retain our cohesion and keep everyone engaged and motivated. Online meetings and socials, including a virtual Christmas cooking event, enabled us to keep the team spirit alive.
And we did our best to make new recruits feel welcome, although they couldn't come to the office or shake hands with their new colleagues. Initiative, creativity and engagement were crucial in terms of making the situation work. Despite everything, we realised most of our plans for 2020, the atmosphere remained positive and sickness absence was lower than ever.

Commercially speaking, 2020 was a good year for SIDN. However, it was also a year that asked a lot of everyone, in their working and private lives. And we are very aware that we are in a privileged position. Our services are internet-based, and demand only increased during a tumultuous year. We were already fully equipped for remote working and our robust finances allowed us scope for further investment. Within the internet industry, that picture is fairly typical, but in other sectors a great many businesses feared for their continuity and a great many workers feared for their jobs.

Time zones don't recognise lockdowns

While internal operations continued to run smoothly, activities on the international stage were challenging. In a normal year, we would visit scores of meetings organised by international bodies and collaborative forums. In 2020, however, such gatherings were held on line. And most were aligned with the host country's time zone, which often meant sessions taking place six hours or more out of step with Dutch time. Naturally, we weren't alone in finding ourselves out of sync. If a conference is fairly short, one can work around a big time difference. However, participation in the prolonged proceedings of ICANN, the IETF and others was rendered almost impossible. Such difficulties were clearly reflected in participant numbers and the progress made with joint projects. Inefficient though it might seem, periodically bringing a large international community together at a given physical location has real advantages. Fortunately, time zones weren't an issue with our own event, SIDN Inspire. The virtual alternative to SIDN Connect was a real success and serves as a good example of an initiative set to continue beyond the coronavirus crisis.

The importance of the internet's infrastructure

Met elke oplossing die het internet bood voor een Every time the internet delivered a solution to an unprecedented problem, our dependence on it grew. Sadly, however, criminals saw that there was money to be made from that situation, leading to a surge in cybercrime. And emphasising once again the importance of a secure and stable digital infrastructure. We continue to play our part in building towards that goal by ensuring that .nl is one of the most secure and trustworthy domains in the world. And, more generally, by investing in a safe, innovative, accessible and future-proof internet. For example, we support numerous promising initiatives (directly and through SIDN Fund), we do research, we participate in national and international forums, and we develop new services that boost the resilience of internet users. The aim of such activities isn't to generate profit, but to utilise opportunities and to help resolve community problems that aren't adequately addressed by others.

Surge in cybercrime emphasised the importance of a secure and stable digital infrastructure.

Back in 2017, that was our motivation for taking a majority interest in Connectis, one of the Netherlands' leading suppliers of secure log-in solutions. We saw the acquisition as a way of invigorating the sluggish digital identities market in the Netherlands. In the years that followed, we invested significantly in the professionalisation and growth of Connectis. Nevertheless, as interest from investors grew, the market developed more quickly than we had anticipated in 2016: competition increased, driving up the level of investment required. Over time, we were obliged to conclude that we were not in a position to compete with international tech investment groups. Therefore, when we received an offer from Signicat – a Norwegian company already active in twelve European countries and aiming for leadership of the European online authentication and digital signature market – we decided to negotiate a sale. Signicat's acquisition of Connectis meant the formation of a major European player capable of achieving even greater social impact. The significant progress made with the professionalisation and growth of Connectis was evident from the increase in the company's value during our years at the helm.

Maximising our impact

At the end of 2020, we decided to transfer further development of CyberSterk to one of our partners, thus ending our direct involvement. The background to our decision was the recognition that we could not ourselves achieve sufficient impact within a reasonable time scale. We will nevertheless continue promoting this security solution for SMEs.

Our efforts to make the delivery and use of online services more convenient and secure will now focus on IRMA: a platform for the privacy-friendly exchange of validated personal and other data, supported by open-source software. The technology features a decentralised architecture that puts users in control of their own data. In 2020, an increasing number of organisations, including major insurance companies and various local governments, started using IRMA.

Divergent interests

The .nl registrars are very important to us. Through the Registrars' Association (RA), we work closely with the registrar community on the promotion of .nl domain names and the security of .nl. Nevertheless, there are some areas in which our views differ from those of the RA and its members. Those differences stem from divergence between the social interests that we pursue and the registrars' commercial interests. Disagreement arises mainly in connection with the activities we engage in alongside our .nl work, with a view to making a positive social impact. Examples include IRMA and Connectis, and the initiatives supported through SIDN Fund. Such activities are undertaken because our mission and strategy are not restricted to the administration of .nl: we are committed to promoting problem-free, opportunity-rich digital living for everyone. Against that background, we had some difficult discussions with the RA in 2020, the final year of the existing cooperation agreement between us. As the year drew to a close, we were nevertheless able to reach a mutually acceptable new agreement. The crux of that agreement is that we will continue to cooperate wherever we can, while respecting each other's independence and autonomy.

Our mission and strategy are not restricted to the administration of .nl.

Looking ahead

We recognise that, despite the emergence of new commercial opportunities, a lot of entrepreneurs, businesses and other organisations find themselves in difficult circumstances. Many of the consequences will not become apparent until 2021. Sadly, those consequences are likely to include business closures. And, even if we are able to resume more normal lifestyles, full social and economic recovery is liable to take years.

Given that previous economic crises have affected development of the .nl domain, we are making allowance for something similar happening in the period ahead.

While 2020 demonstrated the feasibility of working from home, we have no wish to end office-based working altogether. We therefore intend to pursue at least some form of resumption in 2021. The pandemic-related restrictions have emphasised the importance of the personal workplace contact we took for granted before 2020. From asking a colleague to take a look at something, to the spontaneous exchange of ideas that leads to something new: social interaction matters.

On the other hand, I don't expect that, once the pandemic is behind us, we will return to the 'old normal'. Nor would I want that. I envisage more working from home and other remote locations, less travel and fewer traffic jams, and the rise of 'hybrid' conferences, meetings and seminars. More flexibility, leading to a better work-life balance and a rethinking of how we use office space.

Many of last year's lessons were painful, but 2020 taught us a lot. By making use of what we have learnt, we can improve our own lives, our work and our living environments. If we emerge from the crisis with nothing more than regrets, we will have failed ourselves badly.

Towards a more secure internet

As people turned to the internet en masse, 2020 presented cybercriminals with opportunities, which they weren't slow to exploit. Cyber-resilience will therefore be more important than ever in 2021, and we'll be working hard to promote it in various ways. For instance, we'll be using artificial intelligence to identify fake webshops as early as possible. And, because artificial intelligence can also be used in undesirable ways, we'll be working to define an ethical framework for AI in 2021.

A privacy-friendly internet

Unfortunately, we no longer expect the Digital Government Act to become law in 2021. Its provisions are likely to include an accreditation mechanism for digital identification systems that people can use to access the services of governmental and quasi-governmental bodies. The decentralised, open-source IRMA solution will hopefully be one of the systems to gain accreditation, thus giving Dutch people more control over their personal data.

Accreditation of IRMA will give Dutch people more control over their personal data.

A new internet

Meanwhile, we are looking beyond the current internet. The internet that we know today has existed for more than fifty years. When it was developed in the late sixties, no one could have envisaged the way it's used today. Back then, applications such as smart energy grids, remote-controlled robots and unmanned aerial vehicles were the stuff of science fiction. In 2021, our research team, SIDN Labs, therefore plans to continue working with various partners on development of a future internet that can offer a level of trust aligned with the needs of twenty-first-century digital society. We envision an updated or completely redesigned internet that not only is more secure, but also reinforces our digital strategic autonomy and reduces our dependency on big market players and other nations.

An internet for all

Like all crises, the coronavirus crisis amplified existing inequalities. As the digitisation of society gathered pace, people who have difficulty with ICT were put at a greater disadvantage. That concerns us, because we believe that everyone should be able to participate. Therefore, through SIDN Fund, we will again lend our support to various digital inclusion projects in 2021. By doing so, we aim to promote problem-free, opportunity-rich digital living for everyone.

And, in 2021, we will have been doing that for twenty-five years. For it was on 31 January 1996 that we assumed responsibility for administration of the .nl domain from the Centre for Mathematics and Informatics (CWI), which had performed the role since 1 May 1986. Hopefully, it won't be long until we have an opportunity to celebrate our silver jubilee and take a proper look back at twenty-five momentous years. The events of the most recent – by no means least momentous – of those years are described in this annual report. I hope you enjoy it.

Roelof Meijer,
CEO SIDN

01

Rapid growth in .nl registrations

A .nl domain that delivers value and embodies values

Rapid growth in .nl registrations

A .nl domain that delivers value and embodies values

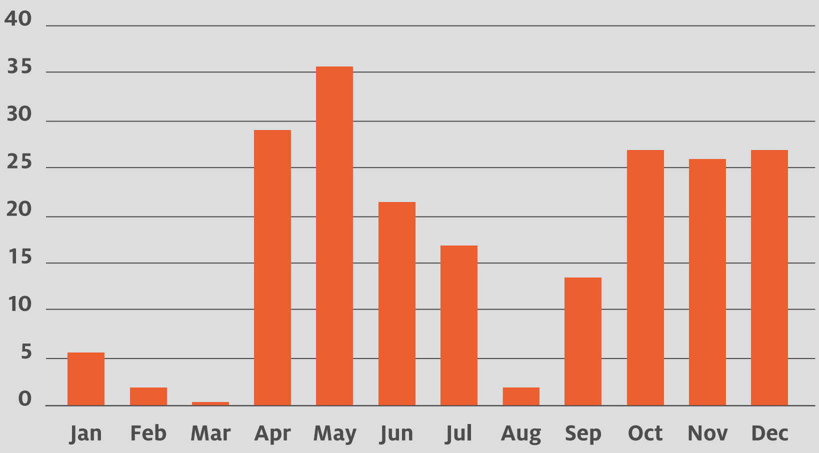
The coronavirus crisis had a major influence on the year. With many businesses pushed to move their activities on line, the .nl domain passed the milestone of six million registered domain names in June – much earlier than had been expected before the pandemic. Our national domain's share of the start-up business market went up as well. Meanwhile, adoption of internet security standards increased steadily, and in partnership with the .nl registrars we were able to further reduce the lifespan of malicious sites. Our registrars also gave our services a very high approval rating.

High availability

In 2020, the availability of our systems deployed within the global Domain Name System (DNS) – the bedrock of our services – was once again 100 per cent. Total availability was achieved despite a sharp rise in the volume of query traffic. Driven by the coronavirus crisis, the number of queries reached 250 million an hour, roughly 10 per cent up on normal. Being dimensioned for peak loads, our infrastructure was comfortably able to cope with the growth. Unsurprisingly, the make-up of the traffic changed as well. Traffic from educational establishments fell off, while consumer traffic rose. Barely any of the maintenance undertaken on the Domain Registration System (DRS) involved perceptible service interruptions, and all the work that did require downtime was completed within the predefined windows.

> *Growth in the second quarter was particularly exceptional.*

Fig. 1 | Development of the .nl domain in 2020 (x 1,000)



Development of the .nl domain

When the COVID-19 pandemic began, new domain name registrations increased, with the result that the milestone of six million registered .nl domains was passed much sooner than previously forecast. Businesses, particularly start-ups, accounted for most of the increase. Growth in the second quarter was particularly exceptional, the net figure being 86,126, compared with 8,020 in the first quarter of the year. Registered on 18 June, the six-millionth .nl domain name was deyogiclub.nl.

Over the year, a total of 994,693 domain names were registered, while 788,252 were cancelled. Net growth was therefore 206,441, or 3.5 per cent. We ended the year with 6,112,308 registered .nl domain names.

Market share

In the Netherlands, the domain name market is largely divided between .nl and .com. Both top-level domains grew in 2020, while interest in other extensions (.eu, .net, .org) declined further. Because many of the businesses that started online in 2020 were targeting regional or local markets, .nl was generally preferred to the more international .com. That helped to push up the new registration preference for .nl from 73 per cent to 80 per cent during the first lockdown. Our overall share of the registered domain name park rose slightly to 64 per cent. During the year, we saw many previously dormant domain names entering use as well. Registrars reported that the proportion of customers buying websites to go with their domain names increased from 30 per cent to 45.

DNSSEC

More than half (55.93 per cent) of all .nl domain names are now DNSSEC-enabled. All the DNS records for those names have digital signatures – cryptographic seals of authenticity. After eighteen months of stagnation, the rate of DNSSEC validation also started rising again in 2020. KPN's decision to activate validation for its fixed-line and mobile customers meant that the technology was enabled for 30 or 40 per cent of Dutch internet users at a stroke. By the end of 2020, roughly half of Dutch internet users were served by validating resolvers. As a result, the Netherlands was no longer lagging behind neighbouring countries in terms of validating resolver use.

During the year, we switched to a new version of the software we use to digitally sign the .nl zone. Transition to the new software had to be implemented with great care, and the whole process took more than a year.

> *The Netherlands is no longer lagging behind neighbouring countries in terms of validating resolver use.*

Developments in the registrar community

The Dutch registrar community is one of the biggest and most diverse in the world. However, a

Fig. 2 | Market share in 2020

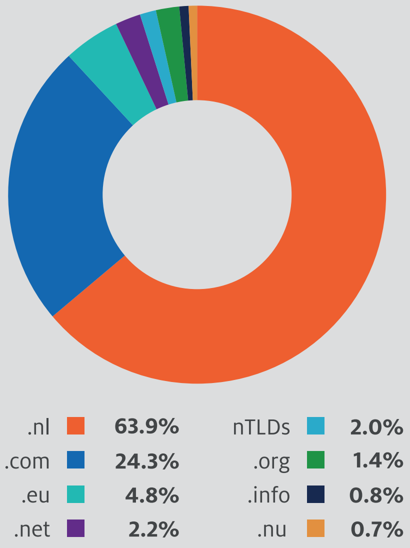


Fig. 3 | Development in the number of DNSSEC-enabled domain names (x 1,000)

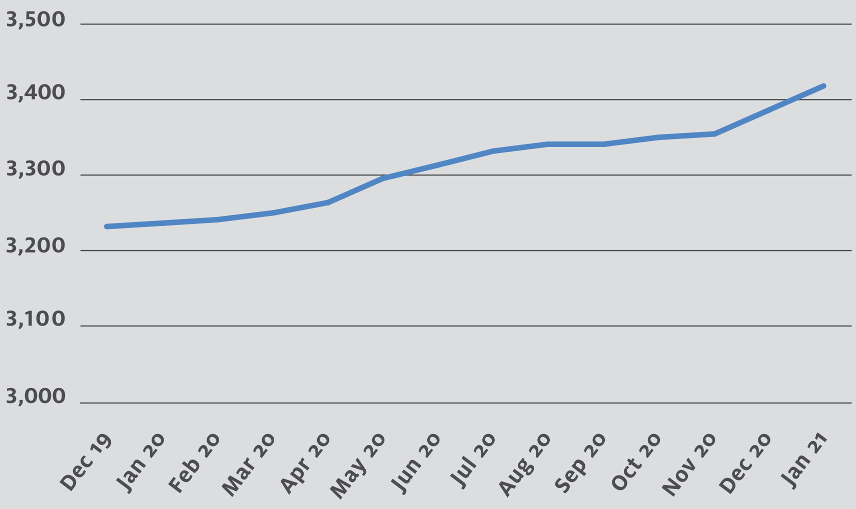
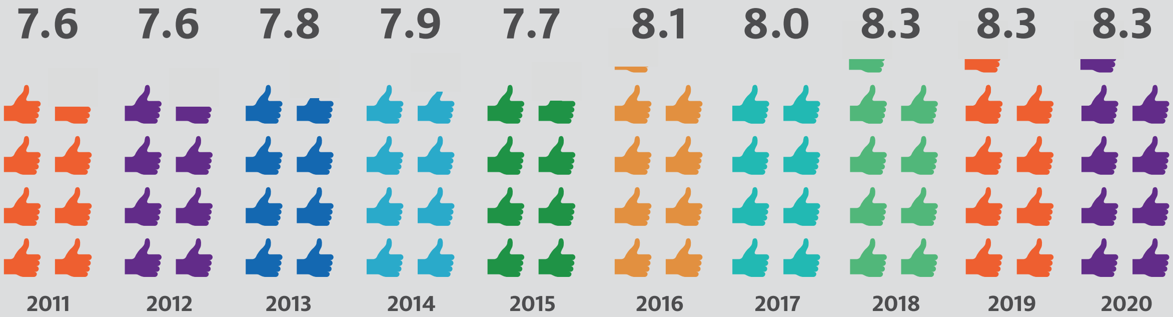


Fig. 4 | Development in customer satisfaction



consolidation trend has been evident for a number of years. That continued in 2020, with the number of registrars falling from 1,209 to 1,156. Acquisitions and mergers enabled several of our registrars to establish themselves as major international players.

Customer satisfaction remains high

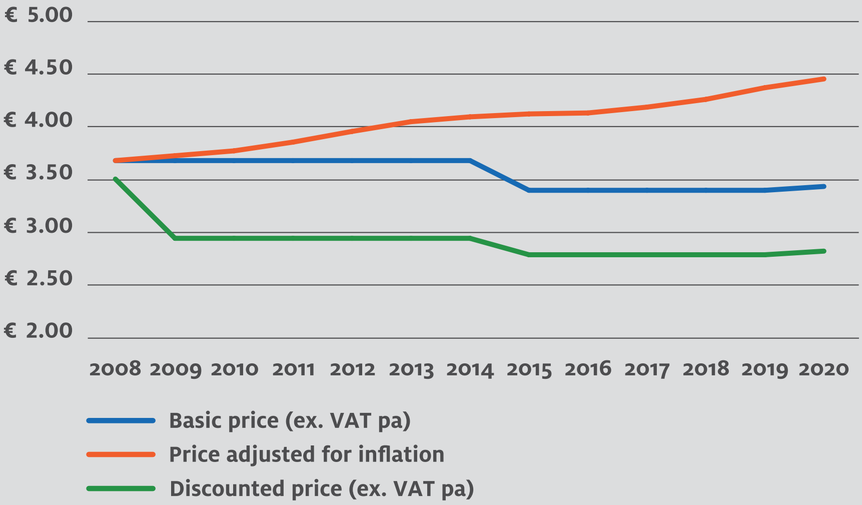
We run an annual satisfaction survey amongst our registrars. In 2020, we matched the high satisfaction score secured in 2019: 8.3 out of ten. As in previous years, approval was highest for personal contact with our Support Department. Respondents were also pleased with the support made available to registrars during the coronavirus crisis, the projects we organised for the registrar community and our activities in the field of co-funded marketing.

Co-funded marketing

In late 2018, we started a co-funded marketing programme. The programme involved giving financial support to qualifying marketing campaigns organised by registrars with the aim of encouraging new .nl registrations and raising .nl's profile as one of the world's most secure and stable zones. Almost all of our ten biggest registrars participated. The focus was on innovative campaigns that have added value for the .nl zone or dovetail with our own strategic goals – campaigns reaching out to new target audiences, promoting new uses or based on innovative approaches, for example. In 2020, it was evident that we and our registrars were becoming increasingly adept at organising such campaigns. Less time was required to assess proposals, and the return on investment was higher. In total, co-funded campaigns generated tens of thousands of new .nl registrations in 2020, at a cost to us of approximately €150,000.

> *We focus on innovative campaigns that have added value for the .nl zone.*

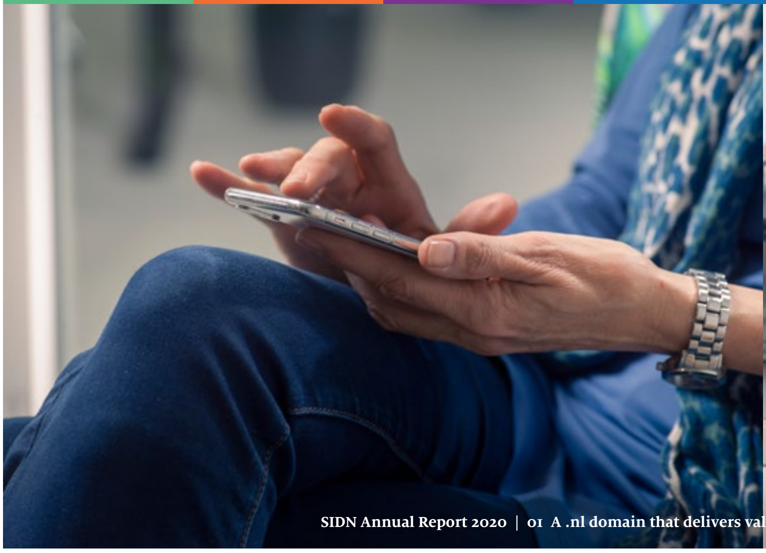
Fig. 5 | .nl price change over time



For confidence online

CyberSterk helps SMEs
Cybercrime represents a significant business risk for SMEs, but many security solutions are too expensive or too complex for smaller businesses. That's why we developed CyberSterk, a user-friendly security solution that provides SMEs with a clear picture of their security status, helping them to do business on the internet with confidence. We know that CyberSterk meets the needs of SMEs. With the aim of enabling CyberSterk to grow more rapidly, at the end 2020 we decided to transfer CyberSterk to one of our project partners.

> Read more on page 20



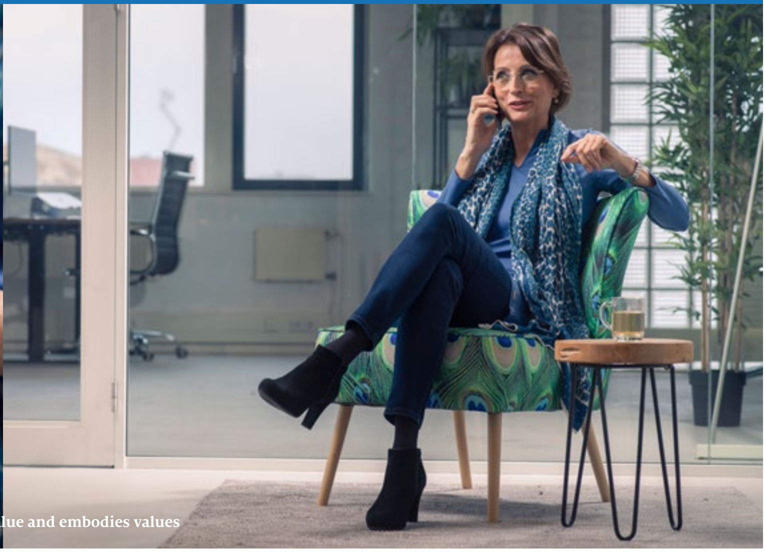
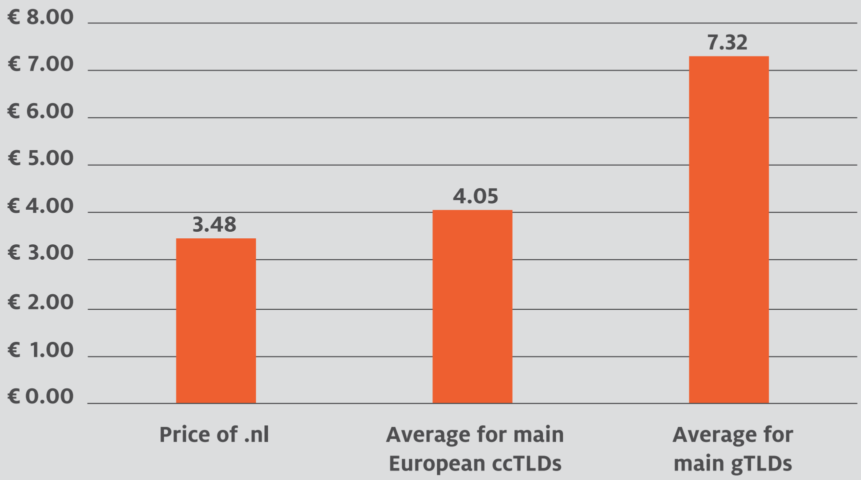


Fig. 6 | Price comparison: .nl and its peers



Price adjustment and reduction in direct debit discount

Because our registrars attach great importance to low prices, .nl registration fees have remained unchanged for a long time. No increase has been made since 2008. However, we now find ourselves in a situation where no substantial percentage-terms growth is expected in the .nl domain, while registrar numbers are falling and costs are rising. Our IT costs generally increase by 3 to 4 per cent a year, for example. Against that background, we took the decision last year to raise prices by 2 per cent per year from 2021 to 2023.

We also announced that our relatively high direct debit discount of 5 per cent, originally introduced to encourage the use of direct debits, would be cut to 2.5 per cent from 2022.

In combination, the two changes mean that the price of a domain registration will rise from €3.40 to €3.48 per year. At that price, a .nl domain name will remain considerably cheaper than a name under almost any other top-level domain available on the Dutch market or elsewhere.

Cooperation with the RA

The .nl registrars form one of our most important stakeholder groups. They are represented by the Registrars' Association (RA), which gives us solicited and unsolicited advice on matters relevant to the registrar community and facilitates cooperation between SIDN and the .nl registrars. We pay the RA's operating costs and work constructively with the RA in fields such as the organisation of registrar services, marketing and communication. However, there are some aspects of our strategy that the RA does not agree with. For example, the RA is opposed to income generated by our .nl activities being invested through SIDN Fund or in advancing the interests of the wider internet community. The announcement of our intention to increase .nl registration fees and cut the direct debit discount led to renewed debate about such issues. We were nevertheless able to agree a framework for continued cooperation with the RA, based on mutual respect for each other's independence and autonomy.

Funding of projects that benefit registrars

Since 2018, we've been investing in projects that help to enhance the .nl domain and have direct commercial benefits for .nl registrars. The projects in question are developed in collaboration with the Registrars' Association. In 2020, we launched the Hosting Infrascan and continued several projects that were already running successfully.

Hosting Infrascan

Many .nl registrars or their resellers provide hosting services. The security of the technical infrastructures used to deliver such services is vital to the security and reliability of the .nl domain. However, getting a hosting platform thoroughly scanned for vulnerabilities is expensive and therefore uneconomical for many hosting service providers. So we teamed up with cybersecurity company ThreadStone to develop the Hosting Infrascan. The service is designed to help hosting firms identify weak spots, so that issues can be resolved. We cover the bulk of the cost of the Hosting Infrascan.

Legal Help Desk

Since 2018, we've been running a Legal Help Desk service for RA-affiliated registrars. The service offers registrars swift, free answers to questions about privacy, terms and conditions and other issues involving ICT and the law. The Help Desk is an independent service facilitated by the legal consultancy ICTRecht.

VPN whitelisting for the DRS

In response to requests from registrars, we set up a VPN whitelist for our Domain Registration System (DRS), enabling secure DRS access from any location.

SIDN Academy

In 2018 and 2019, we organised two successful offline SIDN Academy sessions. The sessions were well attended and well received. However, face-to-face training is not readily scalable. In 2020, we therefore developed an online version of the SIDN Academy, thus increasing the reach and impact of our training activities. The first e-learning course made available through the Academy was devoted to e-mail standards. The SIDN Academy is free of charge for .nl registrars. In due course, we intend to make the programmes available to a wider audience on a low-threshold paid basis. Any income generated will be re-invested in the further development of learning modules.

Fig. 7 | IPv6-enabled domain names

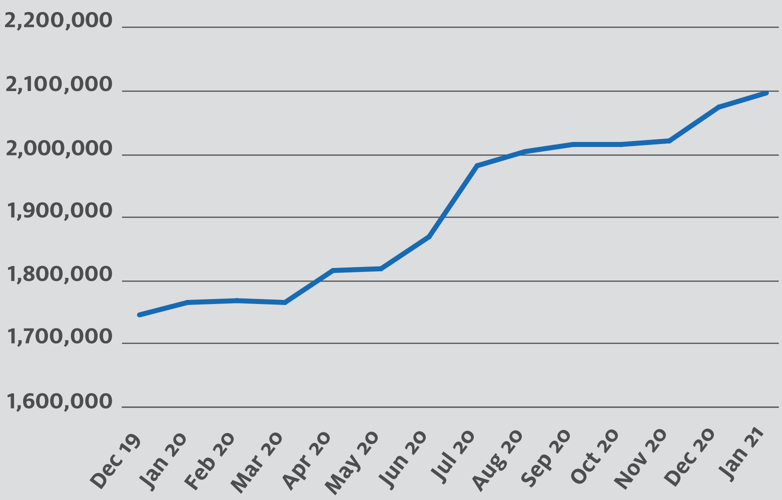
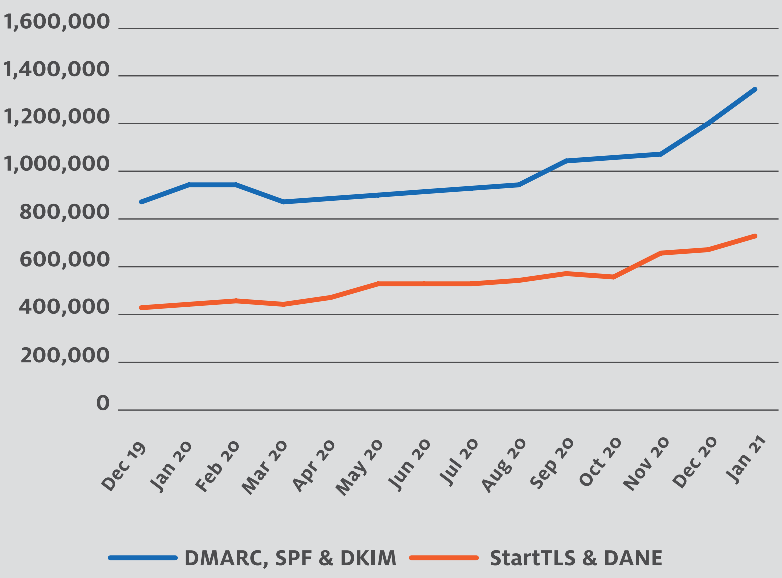


Fig. 8 | Use of e-mail security standards



Registrar Scorecard

The Registrar Scorecard (RSC) incentivises registrars to invest in the value of the .nl domain by enabling secure, modern internet standards for their domain name portfolios. The programme has demonstrably improved the security of the .nl domain. The RSC now has 193 members, including the biggest twenty-five .nl registrars. Together, the participating registrars account for about 90 per cent of the .nl zone.

In 2020, we used the RSC to promote the adoption of IPv6, DNSSEC and the e-mail security standards StartTLS, DMARC, DKIM and SPF. With malicious e-mail practices on the rise, the incentives designed to promote e-mail security standards proved particularly popular. Through the RSC, we returned €1,088,000 to participating registrars in 2020.

Sales funnel on sidn.nl

Back in 2017, we created a sales funnel linked to the domain name lookup utility on our website (the 'Whois'). The funnel directs people who are thinking of registering domain names to suitable registrars. And, if the first domain name they try for is taken, the .nl suggestion tool comes up with alternatives. In 2020, we upgraded the tool to offer extra filter options and deliver even better ideas. For example, we increased the number of (synonym) dictionaries that the tool consults to generate suggestions. So you now get more ideas and better ideas. And the suggestion tool is now automatically enabled whenever you look up a domain name on sidn.nl. We've also made it possible for registrars to embed the suggestion tool on their own websites. The upgraded funnel was delivering roughly five thousand new registrations a month in 2020.

SME survey and campaign

We commissioned market research agency GfK to survey 1,281 small businesses and self-employed professionals for us. Most of the questions were about how much respondents invested in their websites, and how much the websites earned: useful info for the 250,000-plus online start-ups looking to launch successful websites this year. How can small enterprises maximise their chances of doing well? The survey findings were used as the basis for a marketing campaign aimed at SMEs, under the banner 'Do more with your .nl'. Central to the campaign was an online test, which SMEs could use to assess the potential of their .nl domain names.

Our upgraded funnel delivered roughly five thousand new registrations a month.

Dispute Resolution System for .nl Domain Names

In 2020, sixty-one cases were referred to the WIPO Arbitration and Mediation Center under the Dispute Resolution Regulations for .nl Domain Names. Thirty-one of those cases were resolved by WIPO. The other cases were closed, e.g. because the complaint was withdrawn, or because the two sides reached an amicable agreement. Fourteen cases are still under consideration. Our mediators started work on twenty-one cases, three of which are still in progress. In nine of the other cases, successful mediation led to the dispute being settled early.

Complaints and Appeals Board

Normally, the registration and assignment of .nl domain names goes without a hitch. From time to time, however, a registrar or a .nl registrant will be unhappy with a decision that we make. In such cases, the registrar or registrant can appeal to the Complaints and Appeals Board (C&AB). The C&AB is an independent body that also considers complaints about domain name registrations that are believed to be inconsistent with public order or decency. No complaints or appeals were made to the C&AB in 2020. The C&AB's rulings are published on cvkb.nl.

Notice-and-Take-Down procedure

We have a notice-and-take-down procedure, setting out what has to be done if someone contacts us to complain that a website's content is clearly against the law. In the last resort, we can disable a domain name. We received seventy-four notice-and-take-down requests in 2020. Twenty-three of those requests led to us disabling the domain name in question. In the other cases, either someone with more control over the offending content intervened or we decided that the content was not clearly criminal or unlawful.

Transparency Report

The .nl domain is one of the most secure top-level domains in the world, and we work hard to keep it that way. For example, we take the lead on tackling any abuse that involves .nl domain names. Occasionally, the prevention of abuse involves disabling a domain name. And sometimes legal proceedings started by others lead to us being asked to intervene or to share information. The decisions we make in such cases can have serious implications for registrants and others. Therefore, given that transparency is one of the principles that guide our work as operator of the .nl zone, we want to be completely open about the action we take. In that spirit, we started publishing a Transparency Report in 2020, which is updated every quarter.

› Read more on sidn.nl

Vision of internet abuse prevention

We feel it's very important to preserve and enhance the value of our national domain – for which trust and security are vital. Working independently and in partnership with others, we are therefore very active in tackling abuse within the .nl domain and on the internet more widely. Until recently, however, we didn't have a clear written policy on abuse. Following discussions with the Registrars' Association, we decided in 2020 that it was time to change that. Central to our vision is the conviction that our position as operator of the .nl domain implies playing an active role in efforts to prevent improper practices within the .nl zone. The principles that define our role in this field have accordingly been set out in a vision document. The vision document provides clarity for our stakeholders, gives us a framework for our activities and, most importantly, encourages continuing commitment to the prevention of abuse.

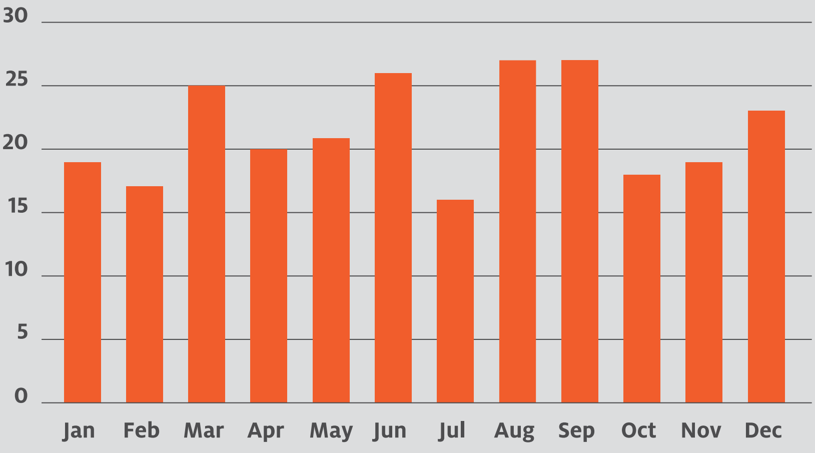
› Read more on sidn.nl

Abuse204.nl

Abuse204.nl ('abuse to zero for .nl') is a programme that we run in partnership with registrars and hosting service providers. Its aim is to tackle abusive activities such as phishing and malware in the .nl zone. Abuse204.nl alerts registrars and hosting service providers to suspected abuse on their networks, enabling them to intervene. Our Support Department maintains an overview and provides support where possible. In the last resort, we can delink a domain name's name servers, making it impossible to reach the associated website by using the name. In 2020, we succeeded in further reducing the average lifespan of phishing sites and malware distribution sites, from thirty hours to twenty-two. Before the launch of Abuse204.nl in 2014, the average was 144 hours.

We succeeded in further reducing the average lifespan of phishing sites and malware distribution sites in 2020.

Fig. 9 | Average up-time of phishing sites and websites with malware in hours



Other registry services

As well as being the registry for .nl, we provide registry services for three other top-level domains: .amsterdam (City of Amsterdam), .politie (Dutch National Police) and .aw (Aruba). In 2020, the National Police extended their registry service agreement with us for a further four years. The force is very happy with our services and values our expertise in domain management. The .politie domain has been active for four years, but is not currently in extensive use. In due course, however, the police plan to employ the domain more widely. For .amsterdam, .politie and .aw, the availability of our domain name resolving (DNS) services was 100 per cent in 2020.

Supervision by the Radiocommunications Agency

In 2018, SIDN was designated an operator of essential services (OES) under the Network and Information Systems Security Act. As such, we became subject to supervision by the Radiocommunications Agency. The Agency carried out its first audit of our work in 2020, using our ISO27001 certification framework as its basis. The findings of the Agency's audits will help us further enhance the security of the .nl domain.

Outlook

Campaign aimed at SMEs

The coronavirus crisis has forced Dutch SMEs and self-employed professionals to become more active online. It will be important to continue highlighting the added value of online activities once the crisis is over. In 2021, we'll be seeking to do that with our SME campaigns, which will focus on the activation of new websites.

Support for registrars

We intend to intensify our programme of support for registrars' marketing activities. We'll also be making relevant market information available to registrars to use in the context of their marketing activities.

Registry services

ICANN is currently preparing for a new gTLD application window, which should open in late 2022. That will provide us with an opportunity to make our expertise and (technical) resources available to organisations seeking support with the technical, legal and policy challenges associated with the application process. We are monitoring developments closely and assessing the desirability of expanding our registry services to include new geo-TLD and/or brand-TLD services.

Anti-Abuse Desk

We are investigating whether we can build on the expertise we've built up tackling abuse in the .nl zone and use it for the benefit of other top-level domains.

For confidence online

The number-one domain for business
There was a surge of domain name registrations in 2020. Many businesses were pushed to move their activities on line, and .nl is the internet domain for doing business in the Netherlands. Because the business community has such confidence in .nl, last year we passed the milestone of six million registrations much sooner than previously forecast. Registered on 18 June, the six-millionth .nl domain name was deyogiclub.nl.

> Read more on page 9

02

Impact in two domains

Online identity en cybersecurity

Impact in two domains

Online identity and cybersecurity

With the aim of promoting problem-free, opportunity-rich digital living for everyone, we are engaged in the development of new products and services in two domains: online identity and cybersecurity. In the first of those domains, we intensified our efforts to build for success with IRMA. Our majority interest in Connectis was sold. In the cybersecurity domain, our focus was on the further rollout of CyberSterk and the proposed transfer to this security solution for SMEs.

Online identity

Connectis

In 2017, we acquired a majority interest in Connectis, one of the Netherlands' leading suppliers of secure log-in solutions, with the aim of giving a boost to the sluggish digital identities market in the Netherlands. We went on to invest significantly in the professionalisation of Connectis's operations and reinforcement of the company's service offering. Meanwhile, however, competition in the sector was increasing. Consequently, Connectis's further development would have required a level of financial commitment that we were unable to make. We therefore sold our majority interest in Connectis to Signicat, a key player on Europe's online authentication and digital signature market, with its roots in Norway.

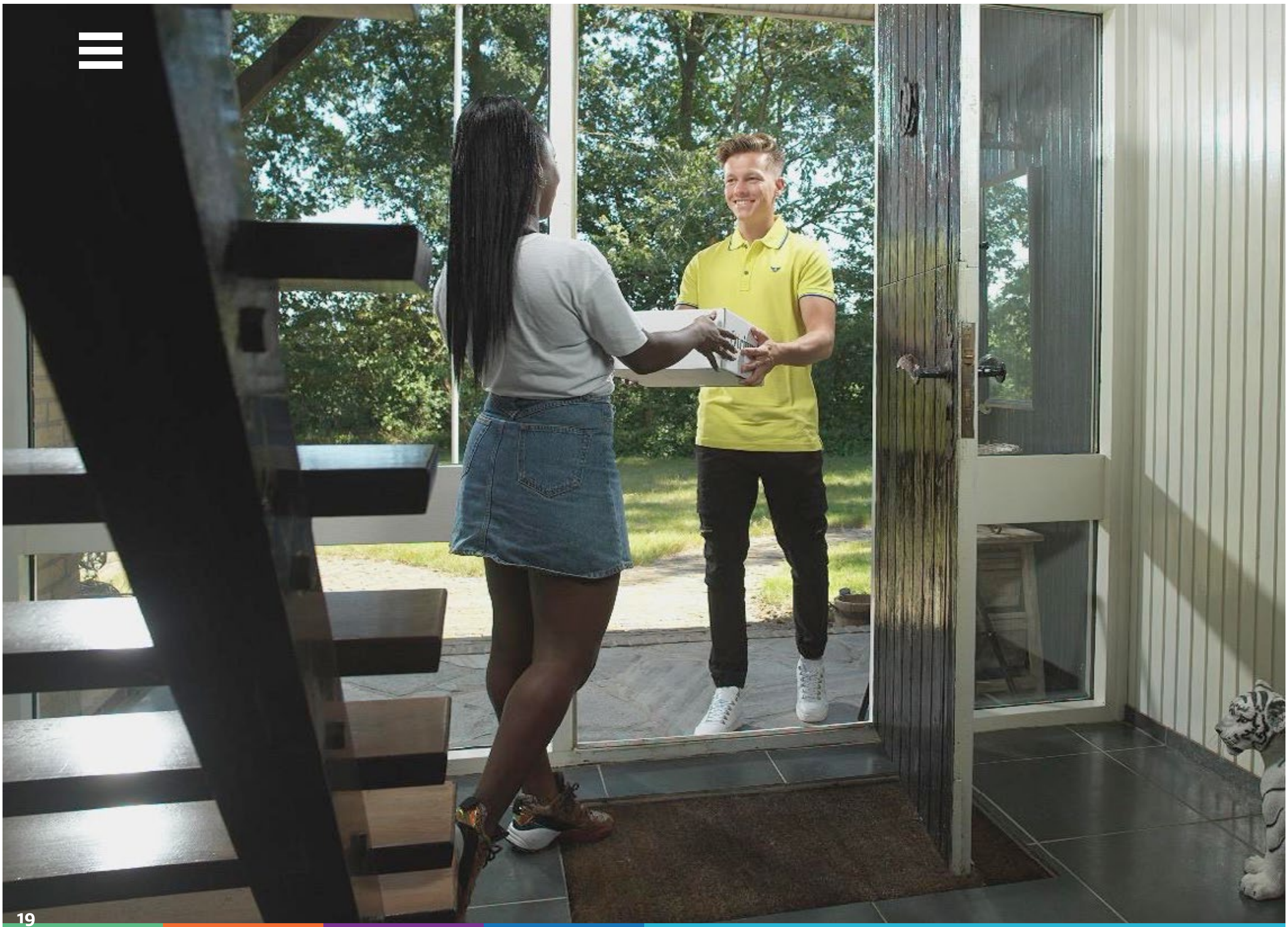
> *We sold our majority interest in Connectis to Signicat.*

Signicat's acquisition of Connectis means the formation of a major European player with the unified experience, expertise and mass to drive accelerated adoption of high-grade online identification and achieve even greater social impact. Since the sale of Connectis, we have had a participating interest in Signicat's parent company, Nordic Capital.

IRMA

IIRMA (I Reveal My Attributes) provides a privacy-friendly way to log in with service providers. During the log-in process, the IRMA app passes on only the information about the user that the service provider actually needs. That might be the fact that the user is over eighteen, or holds a particular bank account, for example. The IRMA app can also be used for digital signing, with the user again identifying themselves using selected personal attributes. So the user shares only the information that's strictly necessary and retains control of their privacy.

IRMA was developed by Bart Jacobs, Professor of Computer Security, Privacy and Data Management at Nijmegen's Radboud University. Management and ongoing development of the software underpinning the service were handled by a not-for-profit foundation called Privacy by Design. We then entered into a strategic partnership with Privacy by Design at the end of 2018. Since 2019, we have been

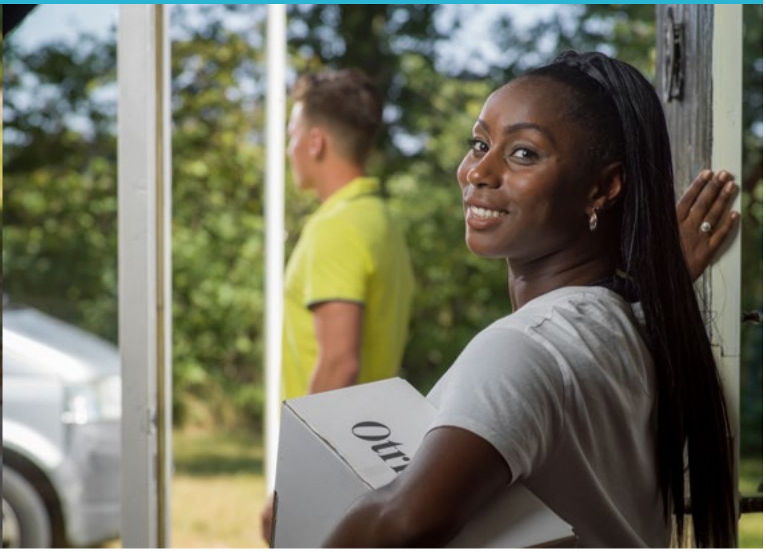


For confidence online

Tackling fake webshops

As people turned to the internet en masse, 2020 presented cybercriminals with opportunities, which they weren't slow to exploit. One popular scam was creating fake webshops. Fortunately, we take an active approach to fighting fake webshops – using artificial intelligence for early detection, for example. Our aim is to uncover fraudulent sites as soon as possible, so that scammers conclude that .nl isn't a lucrative or viable domain to operate in.

> Read more on page 26



responsible for operational matters and have been working on IRMA's further professionalisation and marketing.

In 2020, our focus was on growing the number of organisations offering IRMA logins to their clients, staff and other users. We accordingly developed IRMAconnect, introducing IRMA 'as a service'. IRMAconnect makes it easy for brokers and other organisations to embed IRMA in their web environments, where it can be used for authentication. Various local authorities, health insurers and personal health environment providers started using IRMA during the year.
Identity brokers are also important players in the rollout of IRMA as the authentication medium in the Netherlands. Millions of people use brokers' platforms to access the services of health insurers, government agencies and others. In 2020, Connectis became the first identity broker to offer IRMA support.

We also started lobbying the government to include IRMA as one of the authentication media accredited under the Digital Government Act. IRMA's open format and local personal data storage model appear to be well-aligned with the wishes of the relevant parliamentary committee.

Cybersecurity

CyberSterk

Cybercrime represents a significant operational risk for SMEs. Unfortunately, however, many security solutions are too expensive or technically complex for smaller businesses. In 2019, we therefore introduced CyberSterk: an understandable security solution featuring website and network scans, hardware that detects abnormal internet traffic, plus good practice tips and tests. Once a week, the subscriber's network and website are scanned automatically and the findings are reported on a user-friendly dashboard. Immediate alerts are also sent if acute threats are detected. Regular phishing simulations form part of the service as well. However, CyberSterk doesn't only identify problems; subscribers who don't already have IT partners are additionally given advice on how to resolve the issues we uncover. In short, CyberSterk is a straightforward, affordable security solution that can be a real asset to Dutch SMEs.

We started 2020 with the goal of having about nine hundred paying subscribers by the end of the year, enrolled through about twenty agents, including registrars and others. However, the arrival of COVID-19 prevented us reaching that target. Many SMEs found it difficult to stay afloat, and visiting potential users was not possible for a large part of the year. Against that backdrop, very few CyberSterk subscriptions were sold through registrars. Even after downward adjustment, our targets were not met, with the result that the impact achieved was much less than initially envisaged. In December, we therefore decided to withdraw from further development of CyberSterk.

The arrival of COVID-19 prevented us reaching our targets for CyberSterk.

Nevertheless, we have demonstrated that the proposition is viable and that there is real market demand for a service of this kind. In 2021, CyberSterk will therefore be taken over by Guardian360, one of our partners in the concept's development. Guardian360 is an experienced market player with an extensive client portfolio, capable of taking CyberSterk forward and thus promoting security in the SME sector.
CyberSterk's transfer will also enable us to focus on other projects with a view to maximising our impact on cybersecurity in the Netherlands.

Domain Name Surveillance Service

The Domain Name Surveillance Service (DBS) is a monitoring service that alerts users whenever domain names are registered that closely resemble their own domain names or brand names. With global coverage that includes extensions such as .com, .nl and .webshop, the service provides users with early warnings about registrations that include their brand names, before they go live. Prompt action can then be taken to stop typosquatting, phishing and trademark abuse. Numerous well-known Dutch organisations use DBS, including Achmea, Ziggo, Interpolis and the Dutch national government.

Various major new users came onboard.

The impact of DBS continued to grow in 2020. Various major new users came onboard, including the National Postcode Lottery, the Royal Dutch Touring Club (ANWB) and the Dutch National Institute for Public Health and the Environment (RIVM). Smaller companies, such as food concern Menken Orlando, also recognised the value of online brand surveillance. Another important development was the extension of DBS's coverage to include .co.uk, .gov.uk and other TLDs. We sent more than 4.3 million alerts to users, of which DBS automatically identified 0.7 per cent as suspected phishing scams.

Outlook

IRMA

In 2021, parliament is likely to conclude its consideration of the Digital Government Act. Inclusion of IRMA on the list of authentication media accredited for accessing government services would add considerable momentum to IRMA's rollout. We will also be working to get IRMA adopted by more identity brokers in the year ahead. Finally, we plan to promote use of IRMA by raising awareness amongst end users. Privacy by Design's designers will be joining our payroll, and we will then be taking full responsibility for IRMA's technical development.

Domain Name Surveillance Service

In 2021, we intend to add further features to the Domain Name Surveillance Service (DBS), including a tool that can analyse a website's content and indicate whether the site is likely to be malicious. We'll also be introducing a supplementary Legal Follow-up Module, which will help users take appropriate legal action if they don't have the necessary in-house expertise or capacity. The module will be delivered in partnership with ICT-related legal advice provider ICTRecht. The aim of the move is to widen the scope of DBS from domain name surveillance to brand protection. In line with that realignment, the service may be renamed in 2021. A more modern and convenient user interface will also be developed for DBS.

CyberSterk

Following CyberSterk's transfer to Guardian360, our name will no longer be linked to CyberSterk. However, we will continue to promote the service in the coming year, because we remain convinced that it is an effective answer to a genuine need.

For confidence online

Managing your online identity
IRMA (I Reveal My Attributes) provides a privacy-friendly way to log in with service providers. During the log-in process, the IRMA app passes on only the information that the service provider actually needs – that the user is old enough to watch an adult movie, for example. So the user shares only the information that's strictly necessary and retains control of their online privacy. In 2020, we'll be working to grow the number of organisations offering IRMA logins to their clients, staff and other users. In 2020, Connectis became the first identity broker to offer IRMA support

> Read more on page 18

03

Profit with a purpose

Investment in the Dutch and international internet communities

Profit with a purpose

Investment in the Dutch and international internet communities

SIDN is not a commercial enterprise, but we do endeavour to secure a responsible, positive return on the operation of .nl and our other activities and investments. That is necessary to enable us to continue to innovate and to maintain an adequate financial buffer, and especially to enable us to continue investing in problem-free, opportunity-rich digital living for all.

We are committed to using the income from our activities to enhance the internet's social and economic value to the Dutch and international internet communities. Our research team, SIDN Labs, generates knowledge and develops technologies to increase the reliability of the internet infrastructure. Through SIDN Fund, we support projects that help to make the internet stronger and its users more resilient. And, by playing an active role in international forums and collaborating with numerous other organisations, we contribute to progress in fields ranging from internet technologies and architectures to standardisation, from internet governance and online citizen rights to digital citizenship.

Tackling cybercrime

We lent our assistance to the Port of Rotterdam's FERM cyber-resilience programme, which aims to tackle storage spoofing. That's a form of cybercrime that works like a fake webshop scam, but instead of pretending to sell consumer goods, the scammers use reputable-looking websites to sell non-existent port storage or shipping fuel. Firms that fall for the scams can lose hundreds of thousands. We therefore teamed up with FERM, Rotterdam Port Police and the Public Prosecutor's Office to develop a procedure for disabling spoof sites that have .nl domain names.

> *All members of the Anti-Abuse Network have key functions in the Dutch economy's digital framework.*

Anti-Abuse Network

July saw the official launch of the Anti-Abuse Network, an initiative by SIDN, internet access providers, representative bodies, IT service providers, data centre operators, lobby groups and government agencies. All Network members have key functions in the Dutch economy's digital framework. The Network's purpose is to facilitate and expedite the sharing of information about abusive activities, with a view to improving response measures and the nation's digital resilience. Within the Network, the joint activities are divided across three working groups. The first group's role is schematic planning: deciding who needs what information, in what order. The second group identifies the entities that can play a role and the challenges to be overcome in order to make the internet more secure. Finally, the third working group focuses on clear communication about matters relating to internet abuse.

Hands-on guides

On our website, we published a series of hands-on guides to the implementation of e-mail security standards, such as DKIM, DMARC and DANE, in the two most popular mail server programs, Exim and Postfix. The guides are intended to promote use of the standards and to make mail traffic linked to .nl domains more secure

Podcast series

We produced a podcast series for SMEs entitled Maak jouw bedrijf cyberweerbaar ('How to Boost Your Business's Cyber-resilience'). Presented by Chris van 't Hof, the series explored what SMEs need to know and what they can do to guard against attacks. Every episode was packed with practical advice.

SIDN Labs

Our research team, SIDN Labs, performs large-scale internet measurements and analyses, creates prototypes, contributes to the development of secure, modern standards, and publishes articles, reports and software. By doing so, the team helps to improve SIDN's services and to make .nl stronger and the internet infrastructure more secure. SIDN Labs often collaborates with external partners, such as the University of Twente, Delft University of Technology, the University of Amsterdam, NLnet Labs, SURF and the University of Southern California.

Some of the projects of SIDN Labs in 2020

Measurement tools for DNS operators

SIDN Labs worked with our operations team to develop Anycast2020, a global testbed of twenty virtualised anycast servers that enables us to distribute .nl's DNS traffic across our anycast sites on a more flexible basis. Added flexibility is advantageous when responding to DDoS attacks, for example.
We also developed a new method and tool for measuring the round-trip times of DNS queries. We discovered that Google, one of our biggest clients, was experiencing high latencies (round trips of about 90 milliseconds) when querying .nl's DNS servers. In collaboration with Google and our operations team, SIDN Labs was able to cut that to roughly 25 milliseconds. Details of the research were published in a report.

> *Added flexibility is advantageous when responding to DDoS attacks, for example.*

Shedding new light on centralisation of the internet's infrastructure

We carried out various targeted measurement studies to investigate how the internet's infrastructure is evolving. The studies shed new light on centralisation within the infrastructure. Working in partnership with InternNZ (operator of .nz) and the University of Southern California (operator of B root), we found that roughly 30 per cent of the DNS traffic for .nl originates from internet giants, such as Google and Facebook. We published a peer-reviewed paper describing the research.
In the field of internet routing, we established that 40 per cent of all .nl domain names are protected by RPKI. A higher level of RPKI support is desirable at SIDN and elsewhere, because RKPI is an important security technology for preventing network faults. We also analysed the effects of the coronavirus crisis on the .nl infrastructure and reported on our findings.

Preparing DNSSEC for quantum computers

In the future, we are likely to see the arrival of quantum computers that are much more powerful than the computers in use today. Being so powerful, quantum computers will be able to 'crack' the cryptographic algorithms currently used for DNSSEC. That would be a concerning development, because DNSSEC is a vital security protocol, both for traditional applications, such as e-mail and web browsing, and for IoT applications. We therefore evaluated a number of DNSSEC signing algorithms that may be suitable for use in the quantum computing era. Planning for the transition to quantum-secure algorithms needs to start now, because it can take years to roll out a newly standardised algorithm. Another reason for forward planning is that quantum-secure algorithms are likely to require modifications to the DNSSEC protocol to allow for the use of bigger public keys. We published our work in the form of two peer-reviewed papers.

DDoS Clearing House

Sadly, the internet continues to suffer DDoS attacks. In September, for example, various Dutch ISPs were attacked. Those incidents led to questions being asked in parliament, demonstrating growing awareness of the problem in the community at large. Against that background, we remain committed to increasing the nation's resilience to DDoS attacks. Along with the other members of the National Anti-DDoS Coalition, we refined the prototype for the DDoS Clearing House, a system for automatically sharing data on DDoS attacks in order to improve the response. The system is designed to be easily integrated into member organisations' networks. We also worked with our partners in the EU's CONCORDIA project to visualise and enrich DDoS data and make it available for a future multi-sector European threat information platform.

> *We are committed to increasing the Netherlands' resilience to DDoS attacks.*

Tackling fake webshops

Our fake webshop detector FaDe helps us to get scam sites taken down. In 2020, our Anti-Abuse Desk therefore added FaDe to the toolkit used for abuse prevention on a day-to-day basis. We also improved FaDe by incorporating monitoring functionality that helps us to assess whether our detection models remain accurate. The functionality is based on self-learning algorithms developed by SIDN Labs.

In collaboration with Currence, we ran a pilot, in which FaDe was deployed to scan for the use of iDEAL logos on suspect e-commerce websites. We then investigated whether the identified sites did actually support iDEAL payment, for example. The research will aid the fight against fake webshops in the future.

We also provided input for articles about fake webshops that appeared in mainstream news media, such as Financieel Dagblad.

Another tool developed in 2020 was DEX (the 'Domain name Ecosystem eXplorer'). DEX provides our Anti-Abuse Desk with intuitive visualisations of domain name attributes, such as DNS query data and web crawler data. That makes it easier to identify domain names that are associated with a known malicious site, e.g. domain names that share a TLS certificate with a malicious site. DEX therefore enables our anti-abuse experts to protect .nl users more effectively.

IoT security

SPIN (Security and Privacy for In-home Networks) is an open-source platform that we developed to protect the internet against DDoS attacks where the attackers hijack insecure devices connected to the Internet of Things (IoT), and to provide users with a better picture of what their IoT devices are doing. In 2020, we adapted SPIN to additionally function as an IoT network sensor. Users can upload collected sensor data to our new open IoT data platform, where it is translated into visual representations of their IoT devices' behaviour. The IoT data platform also helps researchers build up a better understanding of IoT device security. In another initiative, we started a study designed to show whether we could use IoT honeypots to gather information about DDoS attacks that utilise IoT devices. We additionally investigated whether we could use machine learning to classify IoT device types on the basis of their network traffic. In collaboration with RIPE experts, we wrote a technical report to assist ISPs with the selection of IoT device protection technologies.

For confidence online

Controlling smart devices

SSPIN (Security and Privacy for In-home Networks) is our open-source software designed to protect the internet against DDoS attacks that make use of insecure devices connected to the Internet of Things (IoT). SPIN gives users a clear picture of what their IoT devices are doing. In 2020, we adapted SPIN to additionally function as an IoT network sensor. Users can upload collected sensor data to our new open IoT data platform, where it is translated into visual representations of their IoT devices' behaviour.

> Read more on page 26

A contribution was also made to SSAC's vision of the interaction between the DNS and the IoT, which we and our SSAC colleagues presented to a plenary session at ICANN68. Finally, we shared our knowledge of IoT cybersecurity by teaching an MSc module at the University of Twente.

Future internet infrastructures

If the coronavirus crisis demonstrated anything, it was the importance of the internet infrastructure. As a result, more attention was focused on issues such as the digital autonomy of the Netherlands and Europe, and the limitations of the current internet. We are therefore studying new types of internet with the potential to complement the existing network: internets that are more secure, stable and transparent, and better aligned with our public values.
In 2020, we connected our network to SCION, an experimental internet with a testbed and an active community. We went on to develop a video demonstrator that utilises SCION and implemented SCION in P4, a language for open programmable router hardware. A technical introduction to SCION was produced as well, and we cooperated extensively with ETH Zurich. Our experience with future internet infrastructures is used for an MSc module that we teach at the University of Twente.

> *We are studying new types of internet with the potential to complement the existing network.*

Responsible internet

In collaboration with various universities and research centres, we devised and developed the concept of a responsible internet. That is an internet that reinforces communities' digital autonomy by increasing users' control over their data while it's in transit. Our thinking on the topic was set out in a paper, and an application was made to the NWO for funding to investigate the concept further.

TimeNL

In 2019, we introduced TimeNL: a public time service based on the Network Time Protocol (NTP). Running at ntp.time.nl, our NTP service can be used for a variety of purposes, such as synchronising system and device clocks. A reliable clock is important for countless applications, including precise determination of who first applied for a given domain name, digital signing of domain names to enhance security (DNSSEC), and communication of the exact creation time of a document or message. In 2020, we made TimeNL available via the Anycast2020 network (any.time.nl), with the result that since December the testbed has been handling about 85,000 NTP queries a second from all over the world.

NTP is an old and relatively vulnerable protocol. Last year, the IETF accordingly ratified a security extension to NTP. The Network Time Standard (NTS), as the extension is known, addresses the flaws in the existing protocol to make NTP more secure. Following the ratification, we adapted our established NTS pilot (nts.time.nl) to bring it fully into line with the RFC.

SIDN fund

SIDN Fund is an independent foundation that we set up in 2014 to promote prosperity and wellbeing in the Netherlands by supporting initiatives that boost the internet's value to the nation. Since then, the Fund has supported more than three hundred innovative projects.

As in 2019, the Fund ran a continuous, year-round call for 'Pioneer Projects': smaller projects seeking grants of up to €10,000. Following careful consideration by the Fund's staff and Advisory Panel, grants were awarded to a total of sixty-nine projects in 2020. The Fund additionally linked up with Culture Eindhoven to organise a joint call with the specific aim of encouraging collaboration between technicians and designers in order to make funded projects more user-friendly and accessible, thus increasing their impact.
Two themed calls were also organised by the Fund: 'Taking Control of Your Data' and 'Internet Against Corona'. The second of those calls was supported by the Ministry of the Interior and Kingdom Relations.

Some of the projects supported by SIDN Fund in 2020

PII Filter

Personally Identifiable Information (PII), such as your name, sex or bank account details, is often shared unnecessarily – when you post on social media or leave a review, for example. In many cases, it happens without you realising it. The PII Filter project is developing software that actively supports users' decision-making and alerts them when a text input dialogue or API request involves unnecessary PII sharing.

COVID planner

The first COVID-19 wave had a serious impact on the organisation of health care. A project was therefore started to help hospitals predict the COVID-19-related demand for care. Demand forecasting can improve the planning of routine care services, help care staff prepare and expedite access to appropriate care. An open-source model was developed, which is freely accessible at covidplanner.nl.

Deep-fake detection

With the naked eye, it's increasingly difficult to tell whether a computer-manipulated video is faked or not, creating serious potential for abuse. A project was therefore set up to build an accessible, free tool for detecting deep-fake videos.

IRMA-meet

With IRMA-meet, you can be sure that your video conference partner is who you think they are. Only people who can confirm their identity using the (free) IRMA app can join protected calls. Authentication with IRMA-meet can be extremely useful for remote oral exams and for medical and other consultations, for example. The tool is available from irma-meet.nl.

> *With IRMA-meet, you can be sure that your video conference partner is who you think they are.*

Liaison with the NCSC

We have a liaison arrangement with the National Cyber Security Centre (NCSC), under which we share knowledge and information with the NCSC and others. Our Security Officer acts as our liaison person.

Contributions to organisations and conferences

We play an active role in various important international forums. Ordinarily, we participate in numerous national and international meetings, helping to organise some of them. However, the coronavirus crisis meant that no face-to-face meetings were held after February 2020.

ICANN

Because of the coronavirus crisis, the three ICANN meetings scheduled for 2020 were held entirely online. There were meetings from 7 to 12 March, from 22 to 25 June and from 13 to 15 and 19 to 22 October, in the time zones of the originally planned meeting locations, namely Cancún, Kuala Lumpur and Hamburg, respectively. Within ICANN, we sit on the ccNSO SOP Committee, the SSAC and the ccNSO PDP working group (the latter being the group tasked with proposing a procedure for appealing against certain types of decision made by IANA). We also represent the ccNSO at the GNSO Council and within the IANA IPR Community Coordination Group. At ICANN68, our representative on the SSAC organised a plenary session on the interaction between the DNS and the IoT. Ahead of each meeting, we worked with the Ministry of Economic Affairs and Climate Policy to organise preparatory sessions for Dutch stakeholders.

RIPE

We have been working with RIPE for many years, and one of our people sits on the RIPE Programme Committee. In 2020, there were two virtual RIPE meetings, from 12 to 14 May and from 27 to 30 October.

IETF/IRTF

The three IETF meetings scheduled for 2020 were also held online. There were meetings from 22 to 27 March, from 27 to 31 July and from 16 to 20 November.

CENTR

We are active members of CENTR, the organisation for European ccTLDs. CENTR organises various meetings, at which members exchange experiences and discuss developments. Almost all the meetings held in 2020 were entirely online. The annual Registrar Day, to which we traditionally invite .nl registrars, also went ahead in virtual form. So too did the CENTR Jamboree, from 25 to 27 May. Within CENTR, we worked with a number of other registries on an eIDAS project, with the aim of making our systems accessible using eIDAS-approved logins.

ECP Annual Festival

Instead of an Annual Congress, ECP | Platform for the Information Society held a three-day online Annual Festival this year, from 17 to 19 November. As usual, we were one of the event partners. SIDN Labs made a presentation on the internet of the future. In addition, various projects supported by SIDN Fund were highlighted during a webinar about how the internet can help fight the coronavirus pandemic.

EuroDIG

We're among the organisations that support EuroDIG, the European Dialogue on Internet Governance. The platform is intended to enable as many stakeholders as possible to discuss internet governance, as a basis for building a better internet for all. EuroDIG 2020 took place online from 10 to 12 June. A unique feature of EuroDIG is that any participant can put a topic on the agenda. The event is all about dialogue and the exchange of ideas; it isn't a decision-making meeting.

SIDN Inspire

On 26 November, we organised the first edition of SIDN Inspire: a livestream event at which a panel of experts discussed the influence of current events on the economy, digital infrastructure, hosting, (cyber)security and other key topics. Various members of the business community also contributed. The event was a great success and was watched by an audience of more than 250.

Academic conferences and publications

SIDN Labs often shares the results of its work in the form of peer-reviewed papers presented at conferences and published in applied scientific research journals. In 2020, for example, we were able to get four of our articles accepted for presentation at prestigious conferences: two at the Internet Measurement Conference (IMC'20) and two at the Passive and Active Measurement Conference (PAM'20). We also had work published in the ACM SIGCOMM Computer Communication Review, the IEEE Communications Magazine and the Journal of Network and Systems Management (JNSM).

Four of our articles were accepted for presentation at prestigious conferences.

Internet Security Platform

The Internet Security Platform is a joint public-private initiative intended to promote internet security. The platform addresses issues such as phishing, privacy and the distribution of child sexual exploitation material on the internet. In 2020, we were again active participants.

Involvement with outside organisations

We support various organisations and projects that promote use of the internet or address its unwanted side-effects. Support is provided both through knowledge partnership and through sponsorship.

Notice-and-Take-Down Working Group

Under the umbrella of the Internet Security Platform, the NTD Working Group oversees the National Notice and Take Down Code of Conduct, introduced in 2008. Our Legal and Policy Manager chairs the group.

Online Child Abuse Expertise Bureau

We are one of the main financiers of the Online Child Abuse Expertise Bureau. The Bureau developed from the Reporting Hotline for Internet Child Pornography. Its mission is fighting the distribution of child sexual exploitation images on the internet. The Bureau additionally received a grant from SIDN Fund for the development of a report desk for child porn in chat groups.

Children safe on internet

Ferdinand Grapperhaus, Minister of Justice and Security, launched a public-private initiative aimed at substantially reducing the use of Dutch servers for the distribution of child sexual exploitation material. SIDN is one of participating organisations.

Alert Online

Alert Online is a campaign run by the government, together with the business and academic communities. Its aim is to boost cybersecurity awareness amongst internet users of all ages and from all walks of life. During this year's Alert Online, we ran a specially developed podcast series focusing on the cyber-resilience of SMEs.

Bits of Freedom

We are one of the sponsors of Bits of Freedom, an organisation that fights for an internet that's open for everyone, where private communication remains private. Bits of Freedom's objectives are closely aligned with our own mission.

DINL

Digital Infrastructure Netherlands is a foundation dedicated to helping the Netherlands remain a leading digital infrastructure hub. DINL represents the companies and organisations that operate the facilities on which the digital economy is based – data centre operators, hosting service providers, internet service providers and others. We were one of the organisation's founders.

ECP

We partner ECP, a neutral platform for the digital society, where the business community, the government and community organisations work together. Its aim is to facilitate and guide the digitisation of Dutch society through cooperation amongst its participants.

NLnet Labs

NLnet Labs is a Dutch R&D institute with a strong international reputation. The organisation develops open-source software and open standards relating to the DNS and routing security. NLnet Labs' DNS software is used on millions of servers all over the world. We are a major co-financier of NLnet Labs' work. SIDN Labs often works closely with NLnet Labs on research projects.

Summer School on Internet Governance

The Summer School on Internet Governance organises an extensive introductory programme on internet governance for students, academics, officials and businesspeople. We sponsor the annual European Summer School on Internet Governance. Because of the coronavirus crisis, the 2020 Summer School had a reduced number of participants and a strict hygiene protocol was applied.

ISPConnect

ISPConnect Nederland is an umbrella organisation that represents more than sixty internet service providers. The association gives its members a voice in the media and in discussions with the government and politicians. ISPConnect participates in debates and working groups, undertakes projects and maintains contact with the media. Many of its members are also .nl registrars. At the end of 2020, ISPConnect merged with DHPA to form the Dutch Cloud Community. Having supported ISPConnect, we intend to support its successor as well, because we believe it's important for the ISP sector to have an effective advocate.

National Anti-DDoS Coalition

We are a member of the National Anti-DDoS Coalition, an initiative by various government agencies, internet access providers, internet exchanges, academic centres, non-profit organisations and banks. The Coalition investigates DDoS attacks and works to stop them in various ways.

Concordia

We belong to Concordia, a European consortium that works to promote an integrated European cybersecurity policy.

2STiC

Through SIDN Labs, we are involved in the 2STiC research programme. 2STiC's goal is to develop and evaluate mechanisms for increasing the security, stability and transparency of internet communications, for instance by experimenting with and contributing to emerging internet architectures, such as SCION.

Abuse Information Exchange

We are one of the organisations behind the Abuse Information Exchange, a platform for sharing information about botnets and other forms of internet abuse in the Netherlands.

Outlook

SIDN Labs

One of our goals for 2021 is to improve coordination between SIDN Labs, SIDN Fund and SIDN, with a view to maximising the impact of our projects.

Anycast

We'll be improving .nl's DNS anycast service in 2021. For example, we plan to build a layer of virtual name servers to supplement our more static name server infrastructure and provide dynamic expansion and contraction capability.

stats.sidnlabs.nl

In the year ahead, we'll make more measured data available on stats.sidnlabs.nl in the form of attractive, interactive visualisations.

Quantum security

Using a realistic testbed in our lab, we'll continue experimenting with quantum-secure DNSSEC algorithms and investigating their potential impact on the DNSSEC protocol.

DDoS attacks

In partnership with the other project members, we'll be running a DDoS Clearing House pilot involving the sharing of real DDoS attack 'fingerprints'. We also plan to refine our prototype so that it can recognise more different types of DDoS attack.

Future internet infrastructures

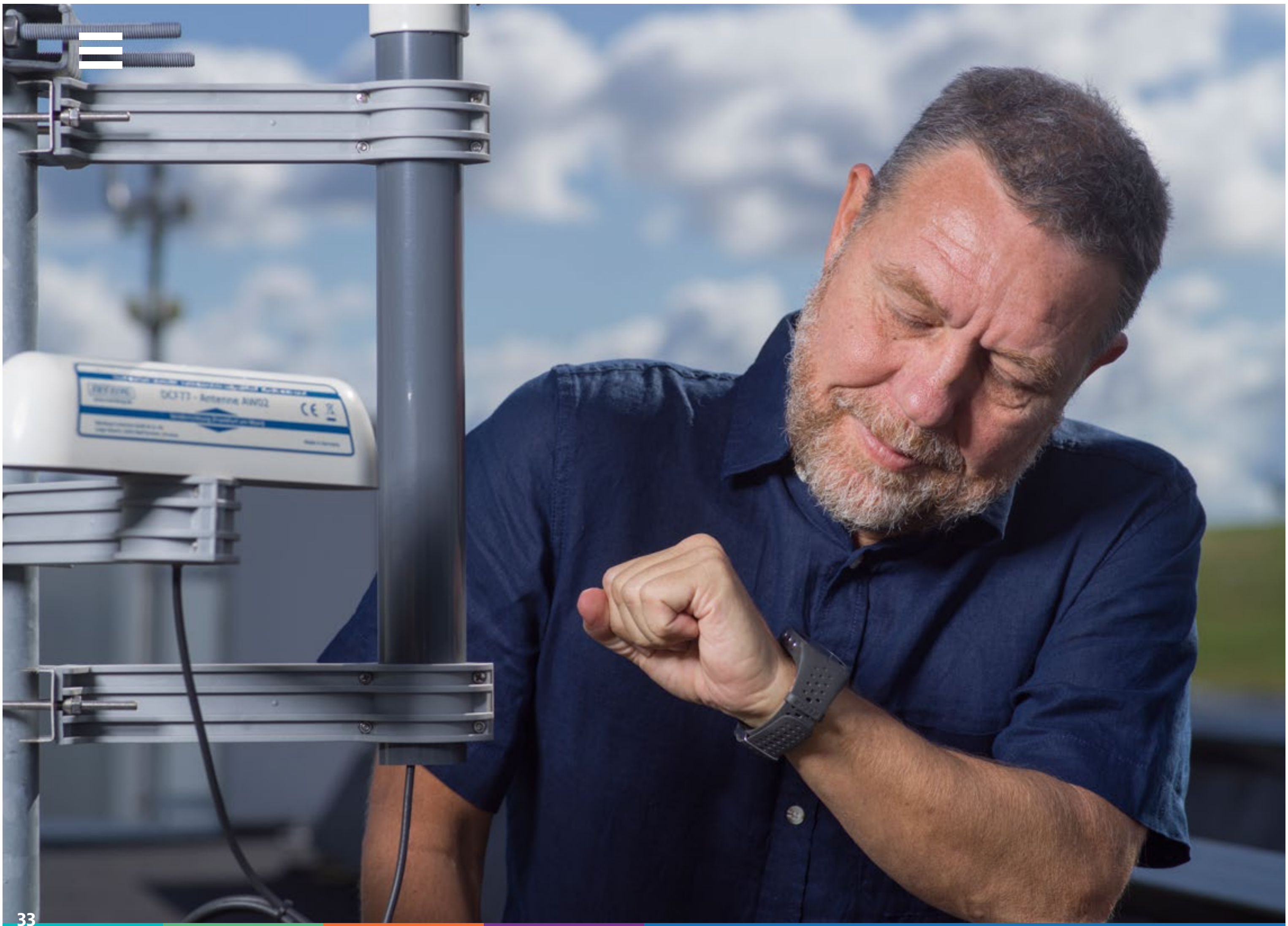
In 2021, we're going to run a pilot with a view to improving insight into how SCION works in an operational setting. We'll also investigate other types of network architecture.

Responsible internet

If we're able to secure funding, seven PhD students will start work on the responsible internet initiative. That will represent a major expansion of the research community looking into secure future internet infrastructures.

Anti-abuse tools

We'll continue refining our anti-abuse tools, such as the logo detector. Possible ways of making the tools more useful to our Anti-Abuse Desk, registrars and other users will also be investigated.

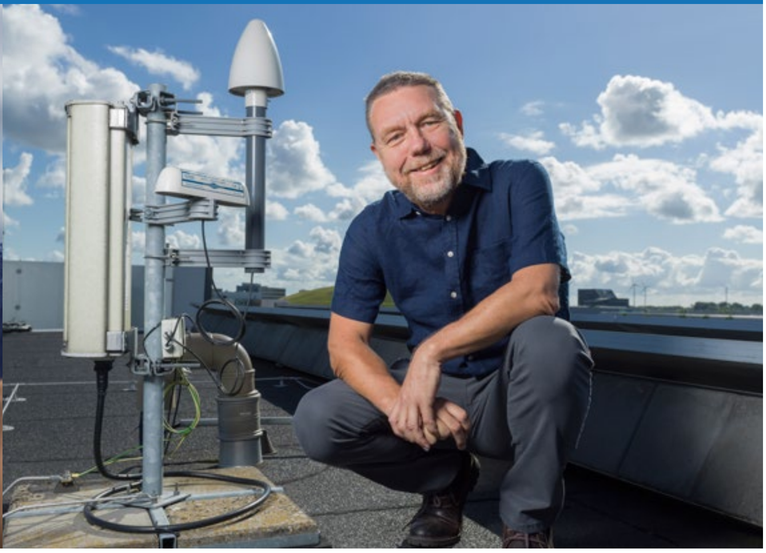


For confidence online

Just in time

In 2019, we introduced TimeNL: a public time service based on the Network Time Protocol (NTP). Running at ntp.time.nl, our NTP service can be used for a variety of purposes, such as synchronising system and device clocks. A reliable clock is important for countless applications, including precise determination of who first applied for a given domain name, digital signing of domain names to enhance security (DNSSEC), and communication of the exact creation time of a document or message. In 2020, we added a security extension to our NTP server.

> Read more on page 28



04

Great creativity and adaptability were needed in 2020

Internal developments

Great creativity and adaptability were needed in 2020

Internal developments

2020 was an exceptional year for our organisation. Pandemic-related restrictions had a major influence on every aspect of our work and on our private lives. Great creativity and adaptability were therefore needed.

SIDN is an organisation with a public role and considerable social influence. Within the company, there is a strong sense that we are working for the good of the nation and the wider world. Our people are highly educated and possess specialist knowledge. We also invest heavily in staff education and training. And we are constantly adapting our working methods to enable ourselves to respond more quickly and effectively to the changing expectations of our customers, the wider community and the internet itself.

Working from home

Time and location-independent working is something that SIDN has always enabled. However, when coronavirus restrictions came into effect in March 2020, everyone had to make an overnight switch to working entirely from home. That placed additional emphasis on internal communication and on staff members' individual needs. As well as providing everyone with suitable equipment, we took steps to ensure that everyone had a home workstation that was appropriate in occupational health and safety terms. Travel allowance payments were suspended and replaced by an allowance in respect of the extra cost of working from home.

> *The pandemic placed additional emphasis on internal communication.*

Workforce and sickness absence

We worked hard to enhance our position on the labour market in 2020. For example, we restyled our 'Working at SIDN' site, developed an internship and student placement policy, and improved our preboarding and onboarding process. Those steps helped us to welcome thirteen new staff members. We ended the year with a workforce of 113 (102 FTEs). Of those, 32 per cent were women and 68 per cent men. Although the coronavirus crisis caused sickness absence to rise in the country as a whole, our absence rate actually fell, from 5 per cent to 2.5 per cent. Factors behind the fall almost certainly included our policies, the additional emphasis placed on welfare and engagement, and the reduced risk of contracting infectious illnesses, such as flu.

Personnel satisfaction

In March, we carried out a personnel satisfaction survey. The overall satisfaction level was 7.7 out of ten: higher than the level recorded in the previous survey (2017), and well above the benchmark. Enthusiasm was also up on 2017, at 7.6, but engagement was slightly down, at 7.5. Various action plans based on the survey findings were formulated and put in motion.

Personal sponsorship budgets

We offer our staff a broad and generous compensation and benefits package. One element of that package is a personal sponsorship budget that each person can use to support a good cause of their choice. In 2020, the scheme was used to assist the Kidney Foundation, a local senior citizens' orchestra and a wide range of other community initiatives that are important to individual staff members.

Renewal of ISO27001 certificate

ISO27001 is a quality standard for information security. Certification is evidence of a high level of information availability, continuity, confidentiality and integrity. In 2020, we successfully had our certificate renewed for the tenth time.

Development and training

We aim to provide an inspiring working environment and ample opportunity for personal development. Seven per cent of the wage bill is therefore allocated to training and development. Because of the coronavirus crisis, it wasn't possible to provide any organisation-wide staff training courses and fewer courses were followed than in previous years.

> *Seven per cent of the wage bill is allocated to training and development.*

Staff Council

In 2020, our Staff Council gave advice on the sale of our majority interest in Connectis. The Council was also asked to approve various proposals, including a proposed revision to our Staff Regulations. In addition, the Council was kept informed regarding SIDN's annual plan and budget for 2020. A meeting between the Council and SIDN's Supervisory Board took place in September.

Privacy Board

In 2020, as in each year since 2014, our Privacy Board assessed and published a number of privacy policies submitted for consideration by internal departments. Such policies are defined for all activities and processes that involve the processing of privacy-sensitive data, explaining how and why the data is processed. One example is the privacy policy for COMAR, a research project that SIDN Labs ran in partnership with the French registry AFNIC and Grenoble Alps University, with the aim of further optimising anti-abuse processes. All such privacy policies and the associated Privacy Board assessments are published on sidn.nl.

Outlook

Working from home

In line with the relevant guidelines, our staff will again be working from home a lot in 2021. Indeed, we expect that more work will continue to be done away from the office even when the coronavirus crisis is over.

The crisis has underscored the importance of keeping everyone well-informed and involved, of fully facilitating home working and collaboration, and of considering people's welfare. Therefore, when the pandemic-related restrictions are eased, we intend to intensify our focus on good internal communication and cohesion.

We are also considering new approaches for putting our premises to better, smarter use after the crisis. We envisage the office increasingly becoming a place for individuals and teams to meet, collaborate and generate ideas.

Working methods

We want more of our work to be organised in line with the DevOps method. It will therefore be important for our IT staff to broaden their knowledge, so that they are better placed to cover each other's roles and operate more flexibly as a team.

In 2021, we will also be placing even greater emphasis on the use of Agile and Scrum teams throughout the organisation.

Team development

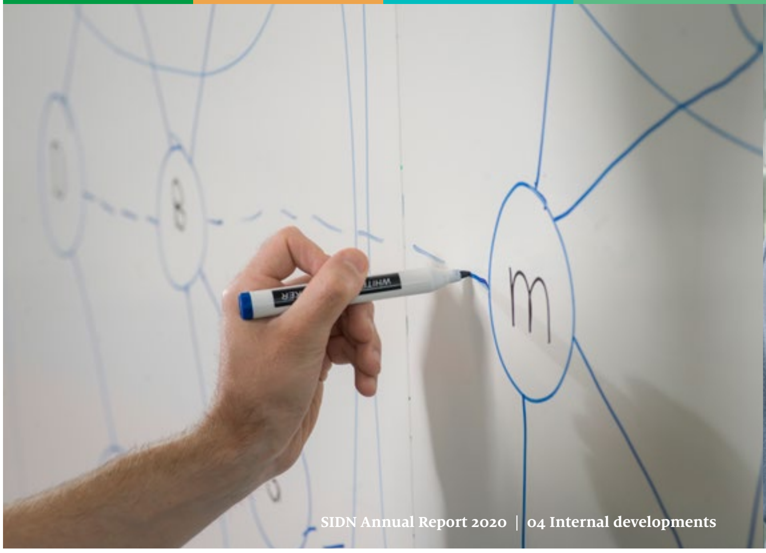
We will continue to promote team development, for example by organising workshops and training sessions devoted specifically to topics such as team effectiveness and coaching leadership.

For confidence online

Working on the internet of the future

If the coronavirus crisis demonstrated anything, it was the importance of the internet infrastructure. As a result, more attention was focused on issues such as the strategic digital autonomy of the Netherlands and Europe, and the limitations of the current internet. We are therefore studying new types of internet with the potential to complement the existing network: internets that are more secure, stable and transparent, and better aligned with our public values. In 2020, we connected our network to SCION, an experimental internet with a testbed and an active community.

> Read more on page 26



05

Report of the Supervisory Board

Paul Schnabel
Chair of the Supervisory Board

Surprisingly smooth transition

SIDN evidently in good organisational health

It was a strange year. While the world struggled with the coronavirus pandemic, SIDN continued to thrive. And, although having everyone working from home has drawbacks, it went remarkably well at SIDN – notwithstanding the fact that, the longer it went on, the clearer it was how important direct contact between colleagues and teams is. SIDN's services were not discernibly affected by the switch to remote working; evidently, SIDN is in good organisational health. Furthermore, when restrictions are ultimately eased, the organisation's premises offer ample scope for people to maintain the recommended physical separation while working.

Most of the Supervisory Board's 2020 meetings were held online as well. On 3 December, the Supervisory Board was strengthened by the addition of Professor Lokke Moerel. Her legal expertise and knowledge of cybersecurity will be an asset to the Board and make her an ideal successor to Peter van Schelven, who steps down at the start of 2021.

The lockdown pushed many businesses and entrepreneurs to find creative new ways of securing an income. The ideas they came up with often involved moving online, or increasing their online activities. As a result, we passed the milestone of six million registered domain names much sooner than previously expected.

SIDN's investment in and commitment to Connectis bore fruit, as the company proved to be a desirable acquisition target for investors. The resulting merger with Signicat has created a major player with the potential to achieve considerable impact at the European level. Moreover, SIDN will be able to use the income from the sale of SIDN's interest in Connectis to reinforce its own contribution to the Dutch internet.

Regrettably, SIDN also had to say goodbye to CyberSterk in 2020. SIDN ultimately proved not to be the right organisation to make a success of the proposition. The effects of lockdown were a contributory factor, certainly in relation to CyberSterk's short-term development. Fortunately, one of our existing CyberSterk partners will be taking the concept forward. We are confident that, once the coronavirus crisis is behind us, there will be increasing demand from Dutch SMEs for the added internet traffic security that CyberSterk offers.

In the period ahead, SIDN will commit strongly to the development and implementation of IRMA. The Digital Government Act, which was still before parliament at the end of 2020, will hopefully soon open the way for government bodies to offer service users privacy-friendly access options. SIDN firmly believes that IRMA represents an ideal, secure solution for use in that context. SIDN has therefore repeatedly and energetically made the relevant political decision-makers aware of the advantages of a system where individual citizens remain in control of their own data.

In 2020, SIDN promoted problem-free, opportunity-rich digital living for everyone in a variety of ways. For example, we actively supported steps to take thousands of fake webshops off line and helped to fight the distribution of child sexual exploitation material. Our financial support for SIDN Fund enabled that operationally independent foundation to lend its assistance to another cohort of promising external projects. Meanwhile, our own research team, SIDN Labs, worked even more effectively in collaboration with other organisational units, and received growing recognition for its research activities.

It is indisputable that the Registrars' Association and SIDN have a common interest in the effectiveness and efficiency of the internet. It was therefore a very welcome development that, at the end of the year, SIDN and the RA succeeded in reaching a new cooperation agreement reflecting that common interest. The Supervisory Board regrets that, in 2020, the RA chose to make the longstanding difference of opinion between SIDN and the RA regarding SIDN's role and responsibilities the subject of public and political attention. While differences may exist in terms of respective interests and views on the role that a registry such as SIDN should play, the SB is confident that the new agreement between the RA and SIDN provides a sound basis for further cooperation.

It is marvellous to see how highly regarded SIDN is on the international stage. Having now been in existence for twenty-five years, SIDN is one the world's largest and oldest country-code registries. The policies pursued down the years, with their focus on service quality and continuity, mean that the organisation is well prepared for the immediate future. Despite the uncertainties of the coronavirus era, SIDN and its committed, expert workforce can look forward with confidence to the next twenty-five years.

Paul Schnabel,
Chair of the Supervisory Board

About the Supervisory Board

The Supervisory Board maintains general oversight of SIDN and its Chief Executive, providing advice as required. The Supervisory Board considers matters such as SIDN's business strategy and the associated risks, realisation of the organisation's objectives and the design and effectiveness of the internal risk management and control systems. Topics addressed in 2020 included pricing policy, the sale of Connectis, expansion of SIDN's involvement with IRMA, cooperation with the RA, evaluation of SIDN Fund and the appointment of a new Supervisory Board member.

Meetings

The Supervisory Board held four routine virtual and face-to-face meetings in 2020. Special additional meetings were held in connection with the sale of Connectis, and several other discussions took place between the CEO and either the entire Supervisory Board or some of its members. In September, the Supervisory Board had a virtual meeting with the Staff Council. There was also regular contact with SIDN's CEO between meetings. Separately, the Supervisory Board's various subcommittees, the Audit Committee, the Selection and Appointments Committee, and the Security and Stability Committee each met at least once.

The following were approved and/or adopted:

- SIDN's Annual Report and Annual Financial Statement for 2019
- Annual reports of the Supervisory Board, the Selection and Appointments Committee, the Audit Committee and the Security and Stability Committee in the context of corporate governance
- SIDN's annual plan and budget for 2021
- Sale of the interest in Connectis Group BV
- Proposals regarding decisions to be taken by SIDN in its capacity as shareholder in SIDN Deelnemingen B.V., such as adoption of the Annual Financial Statement of SIDN Deelnemingen B.V. for 2019

Membership

The Supervisory Board has eight members. Lokke Moerel joined the Supervisory Board on 3 December.

Paul Schnabel, *Chair, Selection and Appointments Committee, Remuneration Committee*
Mark Frequin, *Selection and Appointments Committee, Remuneration Committee*
Simon Hania, *Security and Stability Committee*
Lokke Moerel
Kees Neggers, *Security and Stability Committee*
Jeannine Peek
Peter van Schelven, *Audit Committee*
Willem van Waveren, *Audit Committee*

06

Financial statement

Notes to the Annual Financial Statement

We closed our 2020 accounting year with a positive net result of €3.6 million. The positive result reflected the successful sale of our interest in Connectis. In addition, a one-off supplemented donation of €2.1 million was made to SIDN Fund. The donation was made to enable the Fund to make previously approved but outstanding grant payments. Since SIDN Fund was founded in 2014, our stated intention has been to provide funding of up to €2.5 million per year. By the end of 2020, we had promised a total of €15 million. However, the amount actually donated per year has been the amount needed to cover the project support grants made by the Fund, rather than the full amount promised. The extra donation was made in order to enable the Fund to make project support grants averaging €2.5 million per year and cover its own operating costs.

Operating result

Excluding the donations to SIDN Fund, the operating result for 2020 was €1.6 million (positive), an improvement of €2.9 million on the figure for 2019. The improved operating result reflects higher net turnover and lower operating costs.

The number of registered .nl domain names grew considerably more than expected, resulting in substantially greater turnover than last year. Furthermore, the turnover in 2019 was slightly depressed by a one-off correction, amplifying the effect of the turnover growth in 2020. In the 2020 financial year, a total of €3.2 million was returned to registrars in the form of payment discounts, volume discounts and incentive payments made in the context of the Registrar Scorecard (RSC). The latter item was €0.3 million lower in 2020 than in 2019.

Operating costs

Operating costs, excluding donations to SIDN Fund, were €18.4 million. That is €1.9 million lower than in 2019. Personnel costs fell slightly to €10.2 million, due to reduced expenditure on the hire of temporary staff, particularly for CyberSterk and IRMA. Less was also spent on the hire of temporary Finance personnel, for whom there was less need following the appointment of additional permanent personnel. Hence, lower staff hire costs offset the increased personnel costs associated with permanent staff.

The depreciation charges in respect of goodwill are lower, because of the sale of our interest in Connectis, with effect from 1 April 2020. Excluding donations to SIDN Fund, other operating expenses fell by €1.0 million. The reduction was attributable primarily to the pandemic-related restrictions, which meant that almost no travel or accommodation costs were incurred, and less was spent on the organisation of events. In addition, the operating costs associated with CyberSterk were lower than in 2019.

Financial strategy

The primary aim of our financial strategy is to assure the continuity of our services. That aim is translated into a solvency of at least 60 per cent and a contingency buffer equal to one year's expenditure. At the close of 2020, both our solvency and our equity capital were at target levels.

Our treasury policy is designed to mitigate liquidity risks. To that end, our liquid assets are spread across three Dutch banks. Since 2017, we have additionally held a portfolio of Dutch and German government bonds.

Breakdown of expenditure by strategy

In line with our desire to secure a responsible, positive return, we keep a critical eye on our expenditure. The expenditure associated with each of our strategies in 2020 is analysed below.

1. *Valuable and value-based domain*

This heading covers mainly expenditure on activities linked to management of the .nl domain. The other forms of expenditure included are:

- Direct debit and volume discounts
- Registrar Scorecard incentives
- Funding of projects for registrars
- Our support grant to the RA

2. *Impact in two domains: online identity and cybersecurity*

This heading covers expenditure on IRMAconnect, CyberSterk, the DBS and Connectis.

3. *Profit with a purpose*

The positive return on the operation of .nl and our other activities is used for the benefit of the Dutch and international internet communities. This heading covers expenditure in that context, namely our funding of SIDN Fund, SIDN Labs (and partners), the IRMA platform and community, and our sponsorship of other organisations (including ECP, IDnext, Bits of Freedom and the Reporting Hotline for Internet Child Pornography).

Comparison of actual versus budgeted expenditure in 2020, per strategy

Expenditure on .nl-related activities was lower than budgeted in 2020. That was due mainly to restrictions imposed in the context of the coronavirus pandemic: after mid-March, there was no business travel and all training courses and events were cancelled and/or held online. Expenditure on a number of projects was also lower than anticipated.

Our budget for 2020 envisaged investment in Connectis, IRMAconnect and CyberSterk. However, the sale of our interest in Connectis meant that we more than recovered our investment in the company, and that there was no further expenditure. Some activities linked to IRMAconnect were postponed, due to the slow passage of the Digital Government Act. On the other hand, we scaled up our activities for the IRMA community (strategy 3). Finally, we postponed our planned CyberSterk marketing activities.

The higher-than-budgeted expenditure on strategy 3 is a consequence of the one-off additional grant to SIDN Fund referred to earlier.

Fig. 10 | Budgeted expenditure per strategy in 2020 (€m)

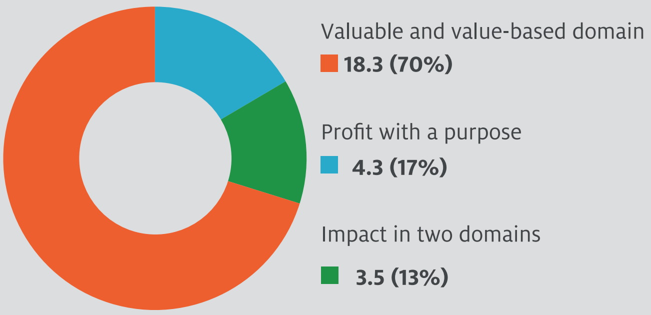
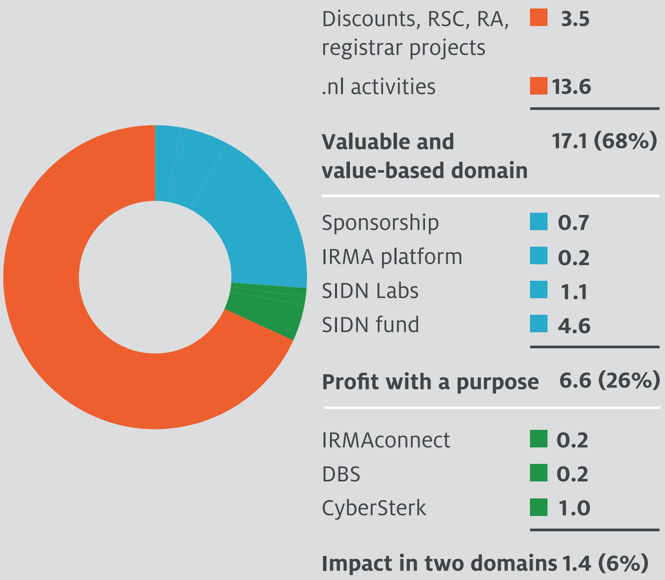


Fig. 11 | Actual expenditure per strategy in 2020, detailed breakdown (€m)



Outlook

In recent years, we have made effective use of a proportion of our accumulated reserves by increasing investment in the internet community, projects for .nl registrars and incentive schemes. Having reduced our equity capital to an appropriate level, we intend to reduce investment and expenditure in the coming years to a level commensurate with the prevailing circumstances.

In 2020, we updated our pricing policy. It was decided that, for the first time in some years, a 2 per cent annual indexation would be applied to .nl registration fees with effect from 1 January 2021. From 1 January 2022, we are additionally reducing the direct debit discount from 5 per cent to 2.5 per cent. The changes are needed in order to protect our long-term financial stability in an environment where our costs are rising year on year, while turnover is barely increasing . That will enable us to continue investing in the security and stability of the .nl domain, as well as in research, projects that have the potential to make the internet better, and activities that the market has so far neglected. We anticipate a slight increase in the number of registered .nl domain names in 2021 and corresponding growth in net turnover.

At the end of 2020, we decided to transfer CyberSterk to one of our partners. The transfer is expected to be completed at the start of April 2021. Meanwhile, we will increase our investment in IRMA. We anticipate a small inflation-led increase in operating costs. In combination, we expect those developments to yield a negative operating result in 2021.

In 2020, we promptly anticipated the government's pandemic-related restrictions and took steps to facilitate working from home. As things stand, we do not expect the pandemic to have any material and/or major financial implications for our operations. Nevertheless, it is plausible that, if the current restrictions remain in place for an extended period, backlogs of work could arise, necessitating a temporary capacity increase. Our intention is to continue the policy adopted in 2020 of monitoring internal and external developments closely and responding as necessary.

Risk management

Vision

Our strategic plan is reviewed on an annual basis and adjusted as necessary. To that end, we perform an analysis of opportunities, threats, strengths and weaknesses, the conclusions of which are translated into a statement of risks and countermeasures. Our risk management activities are focused on:

- The continuity of the organisation
- Assurance of our role as registry for the .nl domain
- Protection of our position and reputation

Governance and organisation

Our Supervisory Board oversees our organisation's strategy, policy and general operational position. The Supervisory Board pays explicit attention to risk management, which is scrutinised by the Board's Audit Committee and Security & Stability Committee.

The Security & Stability Committee supports the Board's supervision of the integrity, confidentiality and stability of our services. The Committee's supervisory tasks also include monitoring compliance with legislation and regulations and with applicable codes of conduct. The Security & Stability Committee additionally considers significant business risks relating to security and stability, the findings of the annual security audit (ISO 27001), the findings of ad hoc narrow-scope audits and penetration tests, and recommendations and other feedback from the external auditor and internal Security Officer.

On the Board's behalf, the Audit Committee supervises the integrity of the organisation's financial reporting, compliance with legislation and regulations and with applicable codes of conduct, and SIDN's financing arrangements.

The management team is responsible for risk policy and risk appetite, and for the direction of control measures. Where information security risks are concerned, the management team is supported by the Security Officer. The Legal & Policy Manager

advises on risks relating to legislation and regulations. SIDN additionally has a Data Protection Officer and a Privacy Board, pursuant to the General Data Protection Regulation.
Line managers are responsible for primary risk management and the associated reporting.

Risks and risk appetite

Our risk management activities have multiple foci, reflecting the main risk areas that we face. Our risk appetite in each area is defined on the basis of careful analysis. The defined risk appetite then determines whether and to what extent a given risk should be taken. The risk appetite definitions provide parameters for decision-making, control measures and course adjustments where additional intervention is needed to keep risks to the desired level.

Dealing with risks

Our risk policy involves the definition of parameters, standards and values with a view to maximising the effectiveness of our efforts to realise our objectives. We consider it important to operate transparently and with integrity.

Main risks and uncertainties

The main risks and uncertainties facing the organisation are itemised below. The developments and control activities associated with each risk area during the year are also summarised.

Strategic risks

The main risks associated with SIDN's strategy stem from the strong dependence on (earnings from) the .nl domain and from the contraction of the .nl market.
Our .nl domain registration services are sold through registrars. Through the Registrars' Association (RA), we therefore work closely with the registrar community on the promotion of .nl domain names and on continuous improvement of the security and quality of .nl. To that end, we entered into a new cooperation agreement with the RA at the end of 2020.

As a consequence of pandemic-related restrictions, we have seen considerable growth in online service provision and .nl registrations. By the close of 2020, there were more than six million registered .nl domain names, substantially more than a year earlier. However, the pandemic's effects on the economy are likely to become apparent in the years ahead. Those effects will inevitably influence development of the .nl domain. Taking all factors into account, we expect the .nl market to remain stable.

At the same time, we are seeking to increase our added value and extend the range of services we offer. Our strategy is therefore to make an impact in two domains: online identity and cybersecurity. That was followed in 2019 by the preparation of two new products – IRMA and CyberSterk – for market introduction. At the end of 2020, we decided to transfer further development of CyberSterk to one of our partners, thus ending our direct involvement. At the same time, we will continue to invest in IRMA, which will be an important focus in the coming years.

Given our limited capacity to influence the end market, our strategic risk appetite is moderate.

Operating risks

The two main risks associated with our operating activities are interruptions to the availability of our services and breaches of the confidentiality or integrity of important data. Such problems could arise from technical and/or human error, or from deliberate (targeted or indiscriminate) human action. A prolonged, large-scale problem in one of those fields has the potential to threaten the continuity of the organisation in two ways. First, by seriously damaging our reputation, giving rise to doubts in political circles and the community at large as to SIDN's legitimacy as the registry for the .nl domain. Second, by leaving us vulnerable to large compensation claims from clients.

Since 2011, we have been ISO27001-certified. That status involves operating an Information Security Management System (ISMS), featuring an annual cycle of business impact analysis, risk identification, risk management and residual risk appraisal, all in accordance with a defined information security policy. The findings, reports and internal and external audits are regularly

Fig. 12 | SIDN's risk appetite

Category	Risk	Low	Moderate	High
Strategic	Dependency on .nl		●	
Operational	Service availability interruptions	●		
	Breaches of the confidentiality or integrity of important data	●		
Financial	Solvency	●		
	Liquidity risk	●		
	Market risk		●	
	Currency risk		●	
	Interest rate risk		●	
	Credit risk		●	
	Bad debt risk		●	
	Damage claims and penalties	●		
Legislation and regulations	Risk of non-compliance with legislation or regulations	●		
Reputation	Reputation risk		●	
Equity capital requirement	Risk of equity capital falling below the defined minimum		●	

discussed, e.g. in our Tactical Security Meetings (TSMs), after which any necessary improvements are implemented. The outcomes are monitored by means of biannual management reviews. In that context, consideration is given to the results of the audits and performance assessments, as well as to the status of audit action points and any security incidents that may have occurred.

The significance of each key process for service continuity is assessed by means of business impact analyses in the context of the ISMS. Our DNS services – the basis of the functionality of registered domain names – are the most critical, closely followed by our registration services, which enable users to register new domain names and to update and cancel existing registrations. Also rated as critical are the Registrar Whois/Is, the power supply, our office ICT systems, our website www.sidn.nl, and our communication and telecommunication systems. With a view to assuring availability, integrity and confidentiality, we have put a wide variety of risk management measures in place, designed to minimise the likelihood of serious problems, and to enable swift corrective action and minimise impact if problems do arise. The measures in question involve, for example:

- The elimination of single points of failure
- Extensive redundancy in hardware, software, connections, external services and expertise
- Logical and physical access control
- Audits and penetration tests
- Vendor requirements
- Internal regulations
- Operations-ready alternative premises for emergency use
- Crisis and relocation drills
- A Privacy Board
- A fully equipped Security Operations Centre

Our operating risk appetite is low in relation to interruptions to the availability of our services and to breaches of the confidentiality or integrity of important data.

Financial risks

- *Solvency*
  Solvency is equity capital expressed as a percentage of the balance sheet total. Between the close of 2019 and the close of 2020, solvency fell from 68.3 per cent to 66.4 per cent. The drop mainly reflects the donations to SIDN Fund outstanding at the end of the year and our increased levels of activity. The closing solvency figure remains above the defined minimum of 60 per cent.

- *Liquidity risk (including concentration risk)*
  Liquidity risk is the risk of having insufficient liquid assets to cover our (annual) expenditure. It incorporates concentration risk: the risk that dependency on a single bank could impair our ability to immediately access our liquid assets. The balance of our liquid assets at the end of 2020 was €27.7 million, up €10.1 million on the close of 2019, due to the sale of our shares in Connectis. In recent years, our liquid assets have also been buoyed by improved cash flow supported by increasing use of annual registration periods for .nl domain names. Our liquid assets are amply sufficient to cover our annual expenditure. Concentration risk is addressed by having our liquid assets spread across three Dutch banks.

- *Market risk*
  Market risk is the risk of our government bonds and/or other securities decreasing in value. Our portfolio of Dutch and German government bonds was acquired with a view to holding the bonds until maturity. If circumstances should necessitate disposal of the bonds prior to maturity, we would face the risk of the bonds having diminished in value relative to the date of purchase. Our holdings of other securities are at risk of declining in value. However, we have not detected any signs (trigger events) indicative of such an eventuality.

- *Currency risk*
  Currency risk derives firstly from the risk that our other securities are devalued by movement in the value of the Norwegian krone. Secondly, there is the exchange rate risk associated with transactions in currencies other than the euro. Our .nl services are priced in euros and therefore entail no currency risk. Because we make little use of suppliers that charge us in currencies other than the euro, our purchasing entails very little currency risk either.

- *Interest rate risk*
  Interest rate risk is the risk that our government bonds and/or receivable loans are devalued by movement in market interest rates. Because we intend to hold our government bonds until maturity, the associated interest rate risk is small. The outstanding loan to Connectis Group B.V. was repaid in full in early 2021.

- *Credit risk*
  Credit risk is the risk that a party with whom we have a contract defaults on their contractual obligations, as associated with other securities, accounts receivable, other receivables and liquid assets. Our bad debt risk is modest, because about 75 per cent of registrars pay by direct debit. Our General Terms and Conditions make provision for action to be taken if a registrar does not fulfil its financial obligations. Our policy is to distribute our liquid assets across three Dutch banks, thus mitigating the associated credit risk.

- *Damage claims and penalties*
  This is the risk arising from service interruptions and data confidentiality or integrity breaches. Our General Terms and Conditions limit or exclude our liability for such problems.

Our financial risk appetite is moderate to low.

Legislative and regulatory risks

Changes to national or international legislation and regulations have the potential to affect our organisation and operating processes. We take stock of potentially significant proposed or impending legislative and regulatory changes – e.g. changes in employment law, tax law or data protection law – at an early stage. The impact of any such change is assessed and translated into organisational adaptations, which are then implemented. In view of the potential impact of legislative or regulatory changes relating to our registry role, we have appointed a Legal & Policy Manager with responsibility for that domain. Where necessary and possible, the Legal & Policy Manager seeks to influence the nature of any proposed changes.

We conducted a comprehensive inventory of our personal data processing activities in connection with introduction of the General Data Protection Regulation. Each processing activity was critically examined to determine whether it was consistent with the new legislation. Where necessary, procedures were modified to ensure compliance with the law. We have voluntarily appointed a Data Protection Officer.

Since 2018, SIDN has been designated an operator of essential services under the Network and Information Systems Security Act. As such, we are subject to supervision by the Radiocommunications Agency. Such supervision is concerned specifically with the stability and continuity of our .nl services, which are the subject of periodic audits by the Agency. We are additionally required to inform the NCSC and the regulator of any serious incidents and we have a statutory duty of care, which covers risk control and incident prevention and mitigation. No serious incidents of a kind covered by the reporting requirement occurred in 2020. We are additionally subject to supervision by the Radiocommunications Agency, with whom we have regular liaison meetings.
Our legislative and regulatory risk appetite is low; we endeavour to operate well within the parameters of all applicable legislation and regulations.

Reputation risk

With a view to managing reputation risks, we work closely with our stakeholders, including the .nl registrars, the RA and the Ministry of Economic Affairs and Climate Policy. Where the registrars are concerned, we pursue an active stakeholder-management policy through the RA. We attach great importance to the quality of our services and to the maintenance and elevation of service quality. In that context, we undertake an annual Registrar Satisfaction Survey. We also actively monitor our media coverage.

Contingency buffer

Om de continuïteit van onze organisatie te waarborgen is het van bIn order to assure the continuity of our organisation, it is important that we have an adequate financial buffer to protect against the possibility of losing a large portion of our income. The contingency buffer additionally serves to protect against the financial implications of the materialisation of an identified risk. Moreover, in event of discontinuation, we would require sufficient funds to ensure the orderly winding up and/or transfer of our .nl activities.
In 2020, we recalibrated our financial strategy and redefined our minimum equity capital requirement as a sum equal to our annual expenditure. Our equity capital is currently above the defined minimum. Our Finance Department monitors the sufficiency of our equity capital in relation to the defined minimum and periodically reports its findings.

Consolidated financial statements for 2020

Consolidated balance sheet as at 31 December 2020 (after appropriation of profit)

Fixed assets	**31 december 2020 (in €)**		**31 december 2019 (in €)**	
Intangible fixed assets		50,454		6,021,677
Tangible fixed assets				
Land and buildings	4,789,525		4,968,951	
Machinery and equipment	918,446		816,494	
Other fixed business assets	535,906		574,703	
Tangible fixed assets under development	193,138		47,054	
		6,437,015		6,407,202
Financial fixed assets		5,525,371		3,999,271
Current assets				
Receivables				
Trade receivables	906,709		207,694	
Tax and social security contributions	66,863		383,948	
Other receivables and accrued and deferred assets	1,585,489		948,738	
		2,559,061		1,540,380
Liquid assets		27,719,876		17,577,002
		42,291,777		**35,545,532**

Liabilities	**31 december 2020 (in €)**		**31 december 2019 (in €)**	
Group equity		27,867,528		24,280,705
Long-term liabilities				
Other liabilities		0	442,651	
Short-term liabilities				
Accounts payable	977,009		732,932	
Tax and social security contributions	687,959		480,480	
Other liabilities and accrued and deferred liabilities	12,759,281		9,608,764	
		14,424,249		10,822,176
		42,291,777		**35,545,532**

Consolidated profit and loss account for 2020

	2020 (in €)		2019 (in €)	
Net turnover	20,005,965		18,934,295	
Purchase value of turnover	-42,693		0	
Net turnover		19,963,271		18,934,295
Expenditure				
Wages and salaries	7,512,593		7,338,005	
Social security contributions	847,190		844,949	
Pension contributions	1,236,973		1,167,679	
Other personnel costs	654,608		980,136	
Depreciation	1,017,491		1,821,568	
Other operating expenses	11,698,133		10,596,751	
		22,966,988		22,749,088
Operating result		-3,003,717		-3,814,793
Financial income and expenditure		27,903		41,327
Result before taxation		-2,975,814		-3,773,466
Taxes		-363,593		180,584
		-3,339,408		-3,592,882
Resultaat deelnemingen		6,926,231		-275,434
Result after taxation		3,586,823		**-3,868,316**

Consolidated cash flow statement for 2020

		2020 (in €)		2019 (in €)
Cash flow from operating activities				
Operating result		-3,003,717		-3,814,793
Adjustments for:				
Depreciation	1,016,799		1,739,593	
Movement in provisions	-		201,462	
		1,016,799		1,941,055
Movement in working capital:				
Movement in receivables	-2,974,456		-263,306	
Movement in short-term liabilities	3,159,422		870,179	
		184,967		606,873
Cash flow from operating activities		-1,801,951		-1,266,865
Interest received	-55,694		19,283	
Corporation tax	-		855,925	
Result from participating interests	6,926,231		-	
		6,870,537		875,208
Cash flow from operating activities		**5,068,586**		**-391,657**
Cash flow from investment activities				
Investments in intangible fixed assets	-		-	
Divestments of intangible fixed assets	5,681,201		6,336	
Investments in tangible fixed assets	-757,282		-636,556	
Divestments of tangible fixed assets	692		76,068	
Movement in other financial fixed assets	-		-	
Long-term lending	-		-	
Income from securities	149,678		138,000	
Income from securities		5,074,288		-416,152
Increase / (decrease) in funds		10,142,874		- 807,809

Consolidated cash flow statement for 2020

	2020 (in € 1,000)	2019 (in € 1,000)
Analysis of funds		
Funds as at 1 January	17,577,002	18,384,811
Movement in liquid funds	10,142,874	-807,809
Funds as at 31 December	**27,719,876**	**17,577,002**

07

Directors and officers

Directors and officers as of 31 december 2020

Chief Executive Officer

Roelof Meijer

Supervisory Board

Paul Schnabel, *Chair*
Mark Frequin
Simon Hania
Lokke Moerel
Kees Neggers
Jeannine Peek
Peter van Schelven
Willem van Waveren

Executive Board

Cristian Hesselman, *Director of SIDN Labs*
Arjan Middelkoop, *Commercial Director*
Tuyen Nguyen, *CFO*
Cees Toet, *Operational Director*

Staff Council

Jeroen Roosen, *Chair*
Chris Faber
Jack van Kolck
Martin Sluijter, *Secretary*
Kolette Visser
Thymen Wabeke
Ruben Wubbels

Privacy Board

Karin Vink, *Chair*
Nick Boerman
Jelte Jansen
Chiel van Spaandonk

Complaints and Appeals Board

Hendrik Struik, *Chair*
Peter Blok
Huib Gardeniers, *Secretary*
Sylvia Huydecoper
Thomas de Weerd
Dennis Wijnberg

08

Glossary

Abuse
Use of the internet for an inappropriate purpose. Common forms of abuse include sending spam, phishing and creating botnets.

Abuse204.nl
Abuse204.nl ('abuse to zero for .nl') is a programme that we run in partnership with registrars and hosting service providers. Its aim is to tackle abusive activities such as phishing and malware in the .nl zone. Abuse204.nl alerts registrars and hosting service providers to suspected abuse on their networks, enabling them to intervene.

Access provider
A service provider that enables customers to access the internet.

Agile working
Working in a responsive and adaptive way. In an agile organisation, projects are often divided into small, surveyable periods and there is continuous consultation with the client. The agile working philosophy originates from the ICT industry and makes use of various techniques, most notably the scrum.

Anycast
Global anycast is a proven and effective technology for spreading network load across multiple instances of seemingly the same server. The way it works is as simple as it is effective: a number of servers share a single IP address, making routers 'think' that they are all the same server. IP packages are forwarded to the 'nearest' point. Local anycast differs from global anycast insofar as a number of local nodes are created. A node is a computer or another device connected to a given network, which can only be approached locally. As a result, worldwide DDoS traffic cannot ever reach a local node. The only DDoS traffic that can reach the node is locally generated traffic, which is much easier to control. Local anycast is therefore an effective response to the risk of major DDoS attacks.

Artificial intelligence (AI)
Artificial intelligence, or AI for short, involves the use of computers to perform tasks that normally require human intelligence.

ccTLD
In full: country-code top-level domain. A top-level domain linked to a country, e.g. .nl (the Netherlands), .de (Germany) and .fr (France).

CENTR
An association for the registries that run ccTLDs, including SIDN. It is a forum for discussion about policies that affect ccTLDs and a conduit for communication between the ccTLDs and other parties involved in the internet's (further) development, such as ICANN. See also centr.org.

Complaints and Appeals Board (C&AB)
An independent body to which .nl registrars and registrants can appeal against certain types of decision made by SIDN. The C&AB also considers complaints asserting that a domain name's registration is inconsistent with public order or decency. See also cvkb.nl.

DANE
DNS-based Authentication of Named Entities (DANE) is a protocol for the secure publication of public keys and certificates.

DDoS
A distributed denial-of-service attack is a concerted effort to make a computer, network or service unavailable to its intended user(s). DDoS attacks can be carried out in several different ways.

DEX
Developed by SIDN Labs, the Domain name Ecosystem eXplorer (DEX) provides our Anti-Abuse Desk with intuitive visualisations of domain name attributes, such as DNS query data and web crawler data. That makes it easier to identify domain names that are associated with known malicious websites, e.g. domain names that share a TLS certificate with a malicious site.

Dispute Resolution System for .nl Domain Names
Anyone who registers a .nl domain name is responsible for making sure that the registration doesn't infringe anyone else's rights. That can happen if, for example, the domain name makes use of someone else's brand name, trading name, personal name or organisation name. If a registration appears to infringe someone's rights, a dispute can arise. SIDN's Dispute Resolution System has been set up as a quick and affordable alternative to using the law courts to settle a dispute.

DKIM
DomainKeys Identified Mail (DKIM) prevents e-mail tampering. If the content of a mail message has been altered in transit, DKIM flags it up.

DMARC
Domain-based Message Authentication, reporting and Conformance (DMARC) is a system for telling mail servers what to do with suspect incoming messages. Servers might be advised to delete all such messages, for example, or to forward them to a particular address. DMARC also provides mail domain operators with information about scam mail supposedly sent from their domain.

DNS
Abbreviation of Domain Name System or Domain Name Server. The global DNS is the system and protocol used on the internet to translate domain names into IP addresses and vice versa.

DNSSEC
Domain Name System Security Extensions (DNSSEC) is a suite of extensions to the DNS protocol. It involves the use of cryptographic techniques to prevent cybercriminals diverting internet traffic to fraudulent websites without the users realising. The basic DNS protocol does not provide optimum protection against such threats.

Domain name
A name within the Domain Name System (DNS), the internet's naming system. A domain name such as sidn.nl is made up of several parts: the top-level domain, '.nl', and the second-level domain, 'sidn'.

Domain Name Surveillance Service (DBS)
A monitoring service provided by SIDN to assist with the identification of typosquats and other issues. Users are alerted if a domain name is registered that is similar to their company name or brand name.

Domain Registration System (DRS)
The system that we make available to .nl registrars for registering .nl domain names and managing existing registrations.

Downtime
The time that a website is unreachable or an application is inactive.

ECP
ECP, the Platform for the Information Society, is a vehicle for the business community, the government and social organisations to work together to support the use of ICT in Dutch society. See also ecp.nl.

eID
Electronic evidence of identity, which can be used for gaining secure and reliable access to online public and commercial services.

ENTRADA
An open-source big data platform developed by SIDN Labs for the analysis of large volumes of DNS data. The database that ENTRADA uses contains more than a hundred million DNS queries.

FaDe
A monitoring tool developed by SIDN Labs, which automatically detects fake webshops on the basis of common characteristics.

Fake webshop
An internet site that looks like a normal webshop, but has actually been set up by fraudsters to trick people out of money and/or to steal data.

gTLD
Generic top-level domain: one of the main types of internet domain. Well-known gTLDs include .com, .org and .edu. The introduction of numerous new gTLDs, including .amsterdam, began in 2014.

ICANN
The Internet Corporation for Assigned Names and Numbers is a non-profit organisation that performs a number of important tasks, such as assigning and specifying top-level domains, assigning domain names and allocating IP addresses. ICANN does not manage any domain names itself. That job is delegated to registries such as SIDN (.nl) and Verisign (.com and .net). See also icann.org.

IETF
The Internet Engineering Task Force is an international community of network designers, operators, suppliers and researchers, which develops internet standards. See also ietf.org.

(Internet) extension
Another term for a top-level domain: the last part of an internet address, after the dot, e.g. '.nl' in 'sidn.nl'.

Internet governance
The development and application of shared principles, standards, rules, decision-making procedures and programmes that shape the way the internet is used.

Internet Governance Forum
The Internet Governance Forum (IGF) is an annual gathering of governments, market players and non-governmental organisations, under the auspices of the United Nations. At the IGF, public policy issues are discussed with the aim of ensuring that the internet remains manageable, robust, secure and stable. The IGF does not define policy. See also intgovforum.org.

Internet of Things (IoT)
A development of the internet, where everyday devices, such as thermostats and baby monitors, are connected to the internet and able to exchange data.

Internet Protocol (IP) address
A unique combination of numbers and/or letters. Every computer or server on the internet has an IP address, at which it can be contacted. If you visit www.whatismyip.com you can check the IP address of the device you are currently using.

Internet service provider (ISP)
A business that provides internet access services to other businesses or private individuals. Many ISPs also provide other services, such as e-mail, web hosting and spam filtering.

IPv6
Every computer or server on the internet has an IP address, at which it can be contacted. Addresses are created in accordance with the Internet Protocol. IPv6 is that latest version of that protocol, which supports an almost infinite number of IP addresses. It has been developed to succeed IPv4 (version 4), because IPv4 addresses are running out.

IRMA
IRMA (I Reveal My Attributes) provides a privacy-friendly way to log in with service providers. First, the user 'populates' the IRMA app with validated data, or 'attributes'. Then, during service log-in, the app passes on only the information about the user that the service provider actually needs. So data sharing is kept to the minimum, and the user stays in control of what they share with whom.

Malware
Any kind of malicious software, including computer viruses and worms.

Name server
A computer on the internet, which 'translates' a domain name into an IP address (a unique numeric internet address). The name server is part of the DNS.

NL IGF
A joint initiative by the Ministry of Economic Affairs, SIDN and ECP.
Its purposes are, first, to embed the conclusions of the international Internet Governance Forum (IGF) in national policy and, second, to ensure that the Netherlands has a voice and that Dutch issues are aired within the international IGF.

Notice-and-Take-Down Procedure
A voluntary internet industry code of conduct on dealing with reports of unlawful or illegal website content, such as child pornography, plagiarism, discrimination and selling illegal goods. The code describes the procedure for complaining about the content of a website. A complaint should be addressed first to the provider of the offending content. If the provider cannot be contacted or refuses to take the content down, the matter may be taken up with

the next party in the chain. The chain is as follows:

- Content provider
- Website provider (registrant)
- Website hoster
- Internet access provider
- SIDN (registry)

If all the other parties in the chain have been asked to take down the offending content but have not done so, SIDN can, in the last resort, disable the associated domain name.

NTP
The Network Time Protocol (NTP) is a protocol that computers use to connect to other computers and synchronise their internal clocks.

NTS
The Network Time Standard (NTS) is a cryptographic security extension to the NTP. It provides a framework for the encryption of messages between NTP servers and other devices.

Open source
A development philosophy based on making source material freely available to all. Open-source software is software whose source code is freely available, so that anyone may copy it, modify it or distribute it without having to pay for the privilege.

Phishing
A form of internet crime. It involves sending e-mails and setting up websites that look as though they come from or belong to well-known and trusted organisations, when in fact they are forgeries. The forged messages and sites encourage people to part with information, such as log-in details and credit card details, which the criminals then use for their own purposes.

Registrant
The person or organisation in whose name a domain name is registered. Only the registrant is entitled to receive SIDN's services.

Registrar
An intermediary who acts for a registrant or prospective registrant in interaction with a registry. (The registry for .nl is SIDN.) Most registrars are hosting service providers, internet service providers or access providers.

Registrar Scorecard
An incentive programme for .nl registrars. Participating registrars can qualify for financial incentives by enabling modern internet standards such as IPv6 and DNSSEC for the .nl domain names in their portfolios.

Registrars' Association (RA)
Association that speaks for the .nl registrars in their relations with SIDN and regularly discusses the main features of registry policy with SIDN.

Registry
In full: domain name registry. The register of all the internet domain names under a given top-level domain, or the organisation that manages that register.

Registry service provider
An organisation (typically a registry) that provides registry services for top-level domains delegated to other organisations. For example, we provide registry services for the .amsterdam and .politie domains.

Resolving
Responding to DNS queries.

RIPE NCC
The Réseaux IP Européens Network Coordination Centre is the Regional Internet Registry (RIR) with responsibility for issuing IP addresses in Europe and the Middle East. RIPE NCC is one of the world's five RIRs, the other four being APNIC (for Asia and Australia), AfriNIC (for Africa), LACNIC (Latin America) and ARIN (for North America). See also ripe.net.

Server
A powerful computer with a fast connection, which is set up to provide information. A web server is directly connected to the internet.

Signing
DNSSEC works with digital signatures, known as 'private keys'. For effective security, DNS data needs to be signed with a digital signature and the signature needs to be checked ('validated') by the data user.

Spam
Unsolicited e-mail.

SPF
Sender Policy Framework (SPF) is a technology for preventing mail 'spoofing' (sending mail pretending to be from someone else). With SPF, the authenticity of mail senders is checked.

SPIN
SPIN stands for Security and Privacy for In-home Networks: an open-source platform developed by SIDN Labs to protect the internet and end users against insecure IoT devices in home networks.

StartTLS
A protocol for establishing secure connections between sending and receiving mail servers.

Testbed
A set-up for testing a technical infrastructure.

TLD
Abbreviation of top-level domain. The domain whose name forms the last part of an internet address, after the dot.

Top-level domain
The domain whose name forms the last part of an internet address, after the dot, e.g. '.nl' in 'sidn.nl'.

Typosquatting
A form of internet abuse that takes advantage of the fact that people sometimes make slips when typing web and e-mail addresses. A user who mistypes an address lands on the typosquatter's site. Typosquatting is often associated with malicious activities such as phishing.

Validation
DNSSEC works with digital signatures, known as 'private keys'. For effective security, DNS data needs to be signed with a digital signature and the signature needs to be checked ('validated') by the data user.

Whitelisting
Whitelisting means putting things on a 'trust list'. For example, you can whitelist IP addresses whose traffic can be trusted for forwarding.

WIPO
Arbitration and Mediation Center An independent, international non-profit organisation that arbitrates in domain name disputes and other cases.
See also wipo.int.

Whois
A protocol for retrieving the details of a domain name, e.g. the name and address of the registrant and registrar, from a database. SIDN manages the Whois data for all .nl domain names. See sidn.nl/whois.

Zone file
A text file listing all the domain names in a zone, plus the associated webserver IP addresses.
.

Colophon

Publisher
SIDN
Meander 501
6825 MD Arnhem
Postbus 5022
6802 EA Arnhem
The Netherlands
T +31 (0)26 352 55 00
communicatie@sidn.nl

www.sidn.nl
www.sidnlabs.nl
www.cvkb.nl
www.domjur.nl

Concept and design
Lumen Designers Network, Breda

Text
ARA, Rotterdam

Translations
G & J Barker Translations, Worcester, United Kingdom

Subscribe to our newsletter
www.sidn.nl/newsletter