2019

Annual Report

SIDN — Your world. Our domain.

2019

Content

1

Foreword

Our firm belief

Internet can help build a better world

Fifty years ago, on 29 October 1969, a message was sent from one computer to another for the first time in history. That exchange between the University of California in Los Angeles and the Stanford Research Institute marked the birth of Arpanet, the network from which today's internet developed. Since then, the internet has become a vital infrastructure, accessible to more than half the people on earth. A world without the internet is now unimaginable. Indeed, the internet is now integral to every aspect of modern life. From the way we work to the way we socialise.

To describe the internet as a success would be an understatement. Yet the fiftieth anniversary of that first message was not marked by rejoicing. Because, in the eyes of many, the internet is 'broken'. They point to its darker side: cybercrime and cyberwarfare, the abuse of personal data, the uncontrolled concentration of power in the hands of a few tech giants, the ability of governments to monitor everything their citizens do.

Here at SIDN, we nevertheless firmly believe that the internet can play an important role in building a better world for all. To do that, however, it must remain open, accessible, diverse and secure. That conviction is the basis of our mission: to promote problem-free, opportunity-rich digital living for everyone.

We pursue that mission in three ways. First, we ensure that the .nl domain is secure and trustworthy. It's down to us that the .nl zone is available all day, every day, delivering huge added value to Dutch

society and the Dutch economy. We've been very successful in that role: the .nl domain has long been one of the world's biggest and most secure country-code domains.

Another way we fulfil our mission is by introducing new products and services within the e-identity and cybersecurity domains. Optimal use of the internet depends on the ready availability of e-IDs that are easy and safe to use. And, without effective, accessible security solutions, trust is undermined and the internet's enormous potential can't be fully realised.

Finally, we promote problem-free, opportunity-rich digital living by investing in the Dutch and international internet communities. We're active in national and international governance bodies, technical forums and consortiums. We develop and share knowledge and we support relevant organisations in a wide variety of fields, from internet governance to the technical core of the internet, from privacy to digital skills.

Last year was certainly an eventful one. The .nl domain continued to grow. We made great strides in the development of new services. And we continued our evolution as a modern, innovative and agile organisation. Full details are given in this annual report, which describes 2019 in relation to the three strategic lines identified above. I hope you enjoy it..

Roelof Meijer,
CEO, SIDN

3

01

Vital to Dutch society and the Dutch economy

The .nl domain. Driven by values, delivering value

4

.nl   nTLDs   1.4%

.eu   5.0%   .org   2.0%

.net   .info   0.9%

Vital to Dutch society and the Dutch economy

The .nl domain. Driven by values, delivering value

The .nl domain is extremely important to Dutch society and the Dutch economy. We therefore have a weighty social responsibility, as provider of an essential service. We discharge that responsibility by constantly investing in the quality and security of .nl, for many years one of the biggest, most secure and most reliable country-code domains around.

However, our role and responsibilities in relation to the .nl domain go beyond the administrative and technical registry functions. We believe we have a duty to serve the Dutch internet community to the best of our ability. That's why we devote so much time and energy to tackling the abuse of .nl domain names for unlawful and criminal purposes, for example, and to getting illegal content removed from .nl websites. We also continue to introduce additional services designed to assure the quality and security of .nl and promote the use of open standards that make .nl more secure and accessible. Our registrars are essential partners in all these endeavours.

High availability

Our DNS systems, which form the bedrock of our services, were again 100 per cent available in 2019. Barely any of the maintenance undertaken on our registration system (DRS) involved perceptible service interruptions, and all the work that did require downtime was completed within the predefined windows.

Certain other systems were affected by brief outages during the year. The unusual number of such incidents was attributable to bugs in the firmware provided by external vendors. Consequently, for the
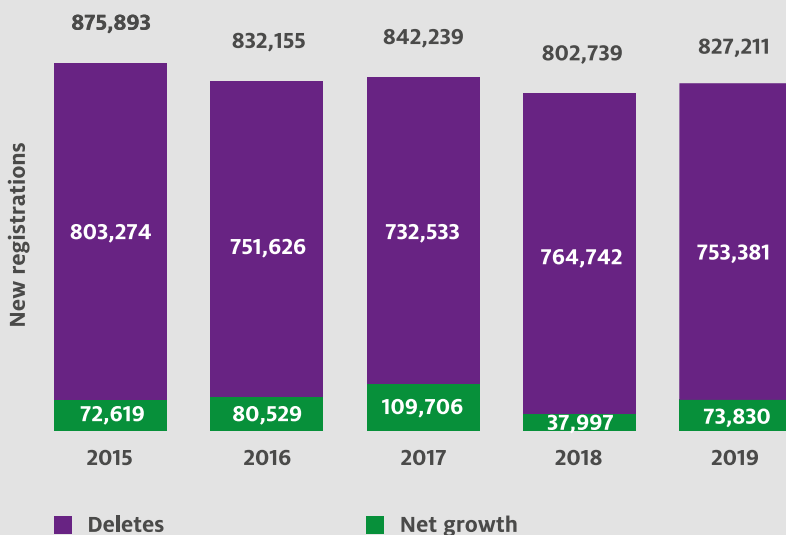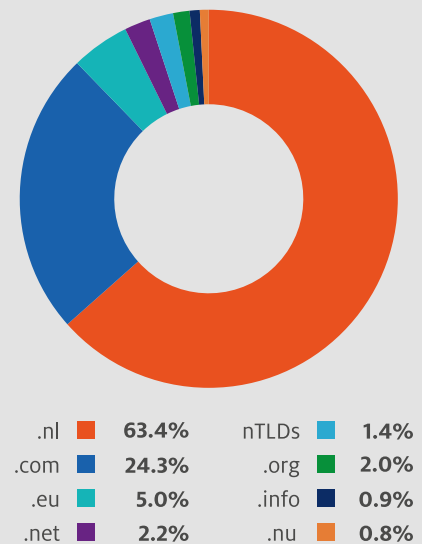
5

Fig. 1 | Development of the .nl domain

	2015	2016	2017	2018	2019
New registrations	875,893	832,155	842,239	802,739	827,211
Deletes	803,274	751,626	732,533	764,742	753,381
Net growth	72,619	80,529	109,706	37,997	73,830

■ Deletes ■ Net growth

Fig. 2 | Market share in 2019

.nl	63.4%	nTLDs	1.4%
.com	24.3%	.org	2.0%
.eu	5.0%	.info	0.9%
.net	2.2%	.nu	0.8%

first time in years, there were three months when we failed to achieve our ambitious target of 99.69 per cent system availability. We were at 99.68 per cent availability in February, 99.59 per cent in September and 99.58 per cent in December.

Towards six million .nl domain names

For the third consecutive year, the .nl domain grew more than forecast. In 2019, the additional growth was largely down to business registrations. Fewer firms were the subject of winding up petitions, and a record number of new businesses – 160,000 – were started. That translated into more registrations and fewer cancellations. A total of 827,211 domain names were registered, while 753,381 were cancelled. For the whole year, net growth was therefore 73,830, or 1.27 per cent. We ended the year with 5,905,867 registered .nl domain names. The milestone of six million domain names is in sight!

Market share

In 2019, numerous new extensions sought to gain a foothold in the market, including .app and .shop. However, none of the new top-level domains have yet secured a significant share of the Dutch market, which remains dominated by .nl and .com. Both of those heavyweights grew again in 2019, with .nl domain continuing to lead the way with a 64.3 per cent market share.

Low prices

Because our registrars attach great importance to low prices, we have repeatedly cut registration fees over the last decade. The basic cost of a .nl registration

Fig. 3 | .nl price change over time

- Basic price (ex. VAT pa)
- Price adjusted for inflation
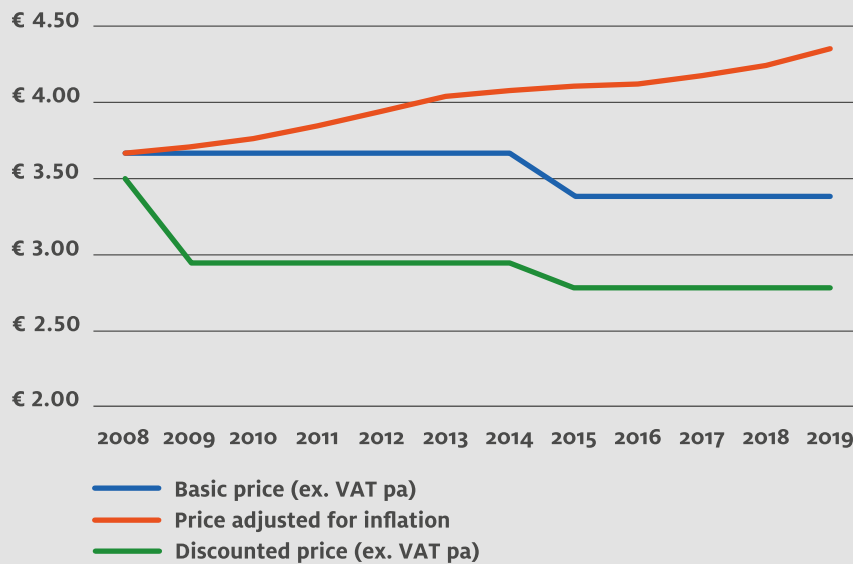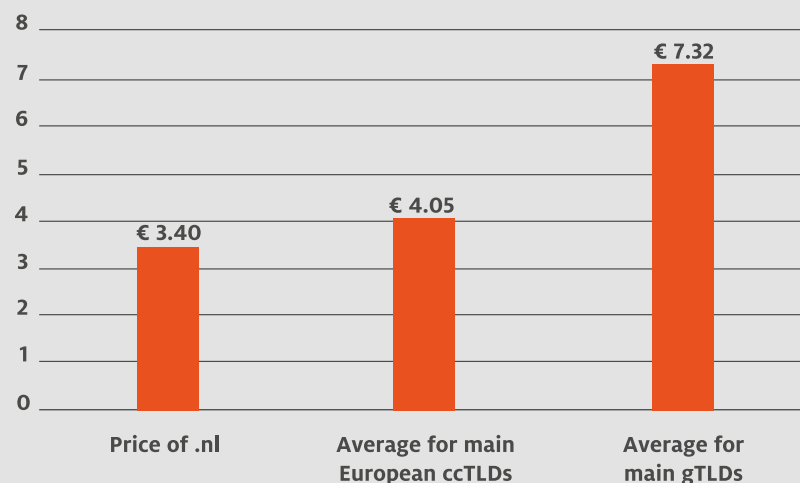- Discounted price (ex. VAT pa)

Fig. 4 | Price comparison: .nl and its peers

N.b. prices converted from local currency.

is roughly 8 per cent lower than it was in 2008, although average prices throughout the economy have gone up by 19 per cent.

Our .nl registration fees remained unchanged once again in 2019. With a basic annual charge of €3.40, excluding VAT, the cost of registering and retaining a .nl domain name are very competitive for registrars. And various discount schemes mean that the actual figure payable can be as little as €2.79. It's therefore much cheaper to register a .nl domain name than to register many of the alternatives.

.nl much cheaper than many other top-level domains.

IPv6
Adoption of IPv6 continues steadily around the world. Fifty countries worldwide have now passed the 10 per cent IPv6 adoption marker. In the Netherlands, user-side adoption stands at 18 per cent. However, that figure is well below those for neighbouring countries. Adoption in Belgium, for example, is currently 51 per cent, while in Germany it's 43 per cent. Sluggish take-up in the Netherlands is mainly down to the biggest Dutch access providers still not offering internet users fully operational IPv6 connections. Sadly, the failure to migrate is starting to impact the Dutch economy by making the Netherlands less attractive as a place for innovation and investment in the Internet of Things (IoT).

On the server side, the situation is fortunately improving. The number of IPv6-enabled .nl domain names remained roughly unchanged in 2019 at 1.77 million, or roughly 30 per cent of the entire .nl domain name park.

We continued working hard to boost IPv6 adoption, by offering an incentive through our Registrar Scorecard incentive programme (RSC), for example. We also organised three IPv6 workshops for .nl registrars under the banner of the SIDN Academy, which proved very popular.

Developments in the registrar community
The Dutch registrar community is the biggest and most diverse in the world. Nevertheless, the number of registrars fell from 1,237 to 1,209 in 2019. Acquisitions and mergers enabled several of our registrars to establish themselves as international players with portfolios of more than a million domain names.

### Customer satisfaction remains high
We run an annual satisfaction survey amongst our registrars. In 2019, respondents gave our services a mark of 8.3 out of ten, the same as the year before. Approval was highest for personal contact with our Support Department, and for the events we organised. Compared with 2018, registrars were more positive about how quickly we made improvements to our systems and processes. Last year, those improvements included rolling out a new registrars' site and enabling scheduled deletion via the Domain Registration System's EPP interface. The survey highlighted Whois data access (restricted in line with the GDPR) and the login procedures for our applications (more time-consuming following security upgrades) as areas where we can improve. As well as gauging satisfaction amongst .nl registrars, we survey users of our other services, such as our registry services and the Domain Name Surveillance Service, to see how happy they are with what we do. Feedback from that client group was also very positive, with an average satisfaction score of 8.5 out of ten.

Co-funded marketing
We supported a number of marketing campaigns organised by registrars to promote new .nl registrations. The focus was on innovative campaigns that had added value for the .nl zone or dovetailed with our own strategic goals. Supported initiatives included campaigns reaching out to new target groups, promoting new uses or based on innovative approaches. The activities illustrated the value of a large and diverse registrar community: it certainly wasn't only the big players that came to us with bright ideas. In 2019, we invested roughly

Fig. 5 | IPv6-enabled domain names
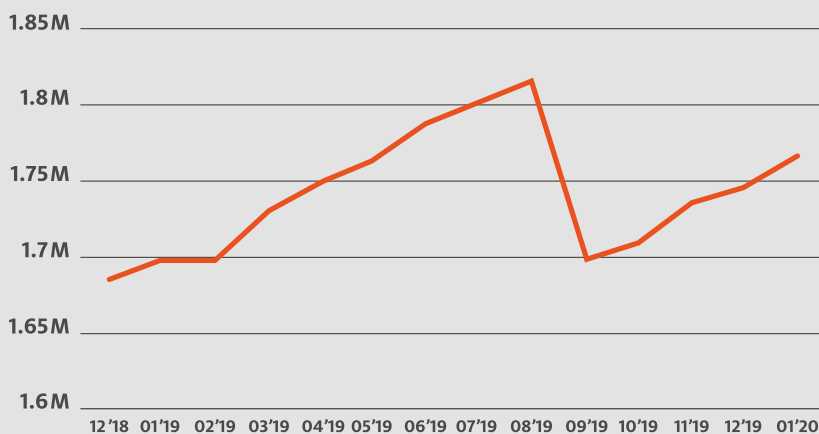
The brief drop in September was due to one major registrar switching to a software package that didn't support IPv6 at the time.

"A win-win arrangement"

Henny Rietkerk
Director of Compra

"We got a mail from SIDN inviting registrars to suggest marketing campaigns. So we sent in a proposal. That led to us developing an e-mail promotion together and me acting as an SIDN representative at Chamber of Commerce Start-ups Day events. My role involved talking to people who are setting up in business, giving advice on choosing a domain name. Of course, there was no guarantee that they would come to Compra to register the names they chose, but we knew that from the start. The project enabled me to talk to prospective customers face-to-face and use my twenty years in the trade to guide them. It was a win-win arrangement: more registrations for SIDN, practical advice for young entrepreneurs and some new customers for my own business. We couldn't have run a campaign like that without SIDN's help. So I'd definitely be interested in doing something similar again. And I think it's really good that SIDN is helping registrars with their marketing. They're giving back to the registrar community. And there are benefits for the .nl domain as a whole."

"Compra's been a registrar since 1996, making us one of the oldest .nl registrars around. When we started, there were about twenty thousand .nl domain names; now there are nearly six million. The .nl domain has become the TLD of the people. None of the new TLDs comes anywhere close. And the marketing initiatives that SIDN is setting up together with registrars should help to keep it on top of the pile."

€100,000 in co-funded marketing. Clear, predefined criteria ensured that the cost per new registration was broadly similar in all the supported campaigns.

An impressive 20 per cent of funnelled leads yield registrations.

Sales funnel on sidn.nl

Back in 2017, we created a sales funnel linked to the Whois utility on our website. 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, alternatives are suggested. With a view to maximising the funnel's effectiveness, we invested heavily in 2019 to refine and extend the suggestion tool involved. An API was added, for example, so that registrars can deploy the tool on their own websites. Commitment to the funnel is reflected in a high rate of conversion: an impressive 20 per cent of funnelled leads yield registrations. Many thousands of leads were directed to registrars in 2019. However, not all registrars have websites that are compatible with our sales funnel. We therefore stopped referring would-be registrants to certain registrars. As a result, about 40 per cent of the registrars who originally enrolled no longer receive referrals.

Chamber of Commerce Start-ups Day

We were represented at various Chamber of Commerce Start-ups Days to help new businesses find good .nl domain names. Using our .nl suggestion tool, we enabled scores of startups to secure their preferred domain names.

Registrar Scorecard

The Registrar Scorecard (RSC) incentivises registrars to invest in the value of the .nl domain. The scheme contributes to the quality of registration data and the active use of .nl, discourages cancellations and promotes investment in security, modern internet standards and abuse prevention. The scheme now has 370 members.

In 2019, the Registrar Scorecard was used to promote the adoption of IPv6, DNSSEC and the e-mail security standards StartTLS, DMARC, DKIM and SPF. Various modifications were made to the scheme during the course of the year. We extended the e-mail security incentive to cover DANE, for example, and we reduced the emphasis on active use, because it is difficult to measure and registrars have relatively little scope for promoting it. In 2019, incentive payments totalling € 1.484 million were made and the programme had considerable impact. The security of the .nl domain was demonstrably enhanced, for instance. Due to its success, the RSC attracted attention from around the world.

Fig. 6 | Use of e-mail security standards
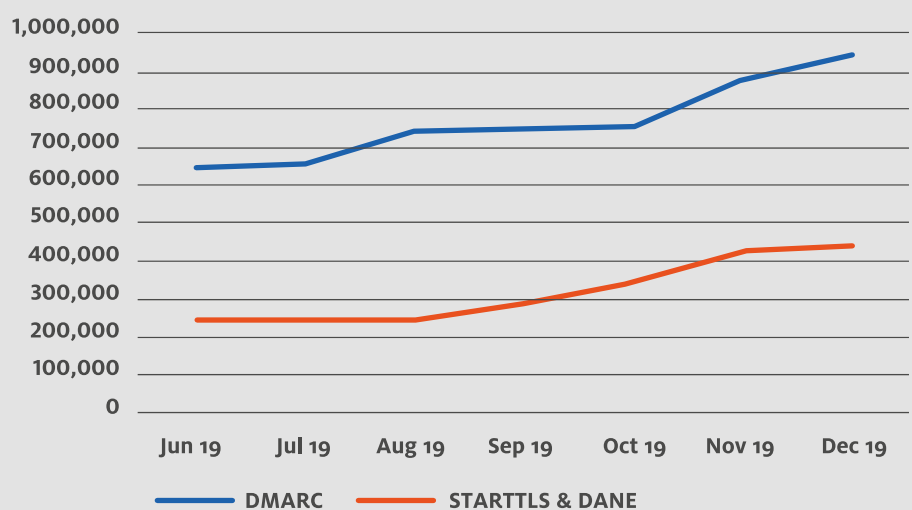
Cooperation with the Registrars' Association

Our registrars are key stakeholders. In their relations with us, they are represented by the Registrars' Association (RA), whose operating expenses we cover. As well as a Management Board, the RA has a Technical Committee, a Legal Committee and a Marketing and Communications Committee. We enjoy constructive and flexible working relations with the RA committees across a variety of fields. Unfortunately, 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 in the SIDN Fund or in advancing the interests of the wider internet community. The RA regards our involvement in such areas as contrary to registrars' commercial interests and would prefer us to confine ourselves to the management of .nl.

> *There are some aspects of our strategy that the RA does not agree with.*

Dispute resolution system for .nl domain names

In 2019, sixty cases were referred to the WIPO Arbitration and Mediation Center under the Dispute Resolution Regulations for .nl Domain Names. Nineteen 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. Eleven cases are still under consideration. Our mediators handled thirty cases. In thirteen of them, successful mediation led to the dispute being settled early.

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 eighteen notice-and-take-down requests in 2019. Eight 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.

Complaints and Appeals Board

A .nl registrar or registrant who is unhappy with a decision made by SIDN can appeal to the Complaints and Appeals Board for .nl Domain Names (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. In 2019, the C&AB received two appeals. Both cases involved a registrar challenging our decision to close their account. However, neither of the appeals was actually considered by the C&AB, because both were deemed inadmissible. The C&AB's rulings are published on cvkb.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 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 2019, we maintained our efforts to drive down the average lifetime of phishing sites and sites with malware. Because we extended our scanning to include various new categories of phishing site and

Fig. 7 | Average up-time of phishing sites and websites with malware
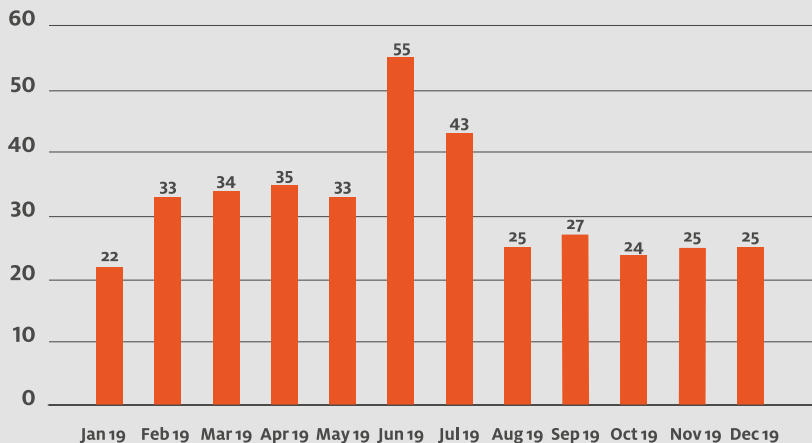
malware at the end of 2018, the average up-time of malicious sites increased in 2019, from eighteen hours to twenty-five. That's still a huge improvement on the situation before the Abuse204.nl started, when problem sites were live for an average of 144 hours. Up-time spikes were recorded in June and July. The spikes were attributable to a handful of cases where we concluded that name server delinking was a disproportionate response. Because the name servers in question were not delinked, the average availability of problem sites went up.

New General Terms and Conditions
We revised our general terms and conditions for registrants and for .nl registrars with effect from 1 May. Most of the changes involved clearer wording or updates to bring the T&Cs into line with current practice. We also added provisions allowing us to disable a domain name if it's clearly being used for an unlawful or criminal purpose. We do that sometimes in order to tackle malware or phishing.

Other registry services
As well as being the registry for .nl, we provide registry services for three other top-level domains: .amsterdam, .politie and .aw. Both the Municipality of Amsterdam and the Dutch National Police extended their registry service contracts with us in 2019. Our expertise and experience with .nl, our secure and stable technical infrastructure and the comfortable working relations we've developed were the main factors influencing the extension decisions.

We also launched RDAP services for .amsterdam and .politie during the course of the year. Short for Registration Data Access Protocol, RDAP is the successor to the familiar Whois protocol that's used to retrieve registration data for domain names. RDAP is a modern internet standard that improves on the Whois in terms of authentication and authorisation, information structuring, and data retrieval and processing. ICANN now requires the use of RDAP for generic top-level domains.
For .amsterdam, .politie and .aw, the availability of our domain name resolving (DNS) services was 100 per cent in 2019.

Outlook

RDAP for .nl
RDAP is becoming the global standard for registration data retrieval. In 2020, we therefore plan to roll out RDAP for the .nl zone, alongside our existing Whois service.

DRS
We plan to investigate whether and, if so, how we can align our Domain Registration System more closely with modern-day user requirements. We'll be analysing the system's processes and procedures, as well as support for current EPP best practices and technical standards.

Abuse204.nl
We're concentrating our anti-abuse expertise in an Abuse Desk within our Support Department with a view to speeding up detection and improving prevention. Our target is to cut the time-to-live of various forms of abuse by 10 per cent.

RSC
We're going to shift the emphasis of our incentive programme. Active use will no longer be incentivised, because the percentage of domain names in active use has remained stable for several years, despite our efforts. The extent to which active use can be influenced by means of an incentive is also debatable, and registrars share our doubts.

Registry services
ICANN is currently preparing for a new gTLD application window, which is likely to open in 2021 or 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 therefore monitoring developments closely and assessing the desirability of expanding our registry services.

> # *"I couldn't believe that such a great name was still available!"*

Nick Verhoog
Owner of bestuurdernodig.nl

"I'm studying Commercial Economics, and I spent some time working as a taxi driver on the side. After a while, I decided maybe I should start my own taxi firm. I thought about calling it Nick's Taxis or something. But one of things we've learnt on our course is that it's helpful for a startup to have a descriptive name. So I started playing with ideas and checking on SIDN's website to see whether the matching domain names were still available. Not surprisingly, the most obvious names were all taken. Then I tried the word 'bestuurder' – Dutch for 'driver' – and the site suggested a name meaning 'driver wanted'. I couldn't believe that such a great name was still available! I found the site's suggestion tool really helpful, because once you've tried ten variations on a name you start to run out of ideas.

One of the things that attracted me to the name was that it's easy to use in adverts. Going on a date and fancy a glass of wine? Driver wanted! Teleconferencing on the go? Driver wanted!"

02

Impact through growth in two domains

E-identity and cybersecurity

Impact through growth in two domains
E-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: e-identity and cybersecurity. Optimal use of the internet depends on the ready availability of identification solutions that are easy and safe to use. And security is an absolute precondition for the internet's continued development. Because, if users can't trust the internet, development is bound to stall.

We've opted for a twin-track approach to the realisation of impact in our target domains: in-house proposition development alongside targeted acquisition. Through our majority interest in Connectis and partnership with Privacy by Design, we are helping to promote secure, privacy-friendly logins. Within the cybersecurity domain, we're deliberately focusing on a small number of socially relevant market segments where solutions are lacking and risks are increasing, such as the SME segment.

e-Identity

Connectis
Since 2017, we have had a majority interest in Connectis, one of the country's biggest suppliers of secure log-in solutions. In 2019, Connectis launched various modified and upgraded features for its platform, including SMS and TOTP-based two-factor authentication, account linking, single sign-on and single log-out, plus a raft of mobile functionalities, including an improved adapter. Connectis also introduced MyConnectis: a secure, user-friendly self-service environment where clients can manage their own identity brokers.

eHerkenning
eHerkenning is the business equivalent of DigiD, one of the Netherlands' most widely used digital ID systems. In the Netherlands, an increasing number of public services can now be accessed only with an eHerkenning token. And Connectis is one of just six approved Dutch token providers.

Against that background, we're marketing Connectis eHerkenning tokens through our registrars. The initiative is enabling registrars to benefit from the opportunities created by our acquisition of a majority interest in Connectis. In 2019, we entered into agency deals with multiple registrars, who have since started selling eHerkenning tokens.

We are enabling registrars to benefit from the opportunities created by our acquisition of a majority interest in Connectis.

IRMA
IIRMA is an identity platform that offers a privacy-friendly way of logging in with commercial and public-sector organisations. With an IRMA login, the user decides what personal information ('attributes') to share, controlling the process with a dedicated phone app. The information shared might include the fact that the user is over eighteen, or holds a particular bank account, for example. IRMA is an

"IRMA eliminates a lot of noise by unifying sources and data."

Hans Niendieker
CEO of Ivido

Ivido is an online platform that enables remote consultation and communication between health care professionals and their clients.

"The care sector is a maze of logins and portals. And it's always the care provider that owns the patient data. So clients have no control over their medical records. With Ivido, it's different: it's the user who's in charge. That same principle – that data belongs to the person it relates to – is reflected in the way IRMA works. IRMA enables the user to create a digital passport, stating what data they're willing to share and what data they don't want shared. That's why we use IRMA to enable secure user logins. IRMA eliminates a lot of noise by unifying sources and data. And, because the information source is reliable, exchanging data is more straightforward."

"We're working with IRMA to improve the user experience. For example, applying for a digital passport was initially a bit of a chore, so we've simplified that process. And we're constantly looking for ways to lower the login threshold."

acronym derived from 'I Reveal My Attributes'. Because information about where the user has logged in and which attributes were revealed aren't shared with any third party, IRMA gives users more control over their privacy. What's more, there is no centralised storage of personal data, making IRMA a neat solution for the identification and authentication challenges facing the health care sector and others. IRMA also provides a basis for increased assurance in authentication processes: an organisation can restrict access to a login page, for example.

With a view to promoting the adoption of IRMA, in August we formed a strategic alliance with Privacy by Design, the foundation behind the technology. Under the arrangement, we now operate IRMA's backend infrastructure, assuring continuity and availability. In 2019, we increased redundancy in the relevant systems, thus making them even more robust and reliable. We also developed services that facilitate third-party use of IRMA and struck deals with the first user organisations.

Cybersecurity

Domain Name Surveillance Service (DBS)
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 numerous well-known Dutch companies with early warnings about registrations that include their brand names, before they go live. The companies can then move swiftly to stop typosquatting, phishing and trademark abuse. The impact of DBS has been growing: in 2019, the number of subscribers rose to 195 and the number of monitored keywords to 425. We sent nearly 370,000 alerts to users, of which DBS automatically identified 4.7 per cent as suspected phishing scams. Revenue from the service increased from roughly €190,000 to about €260,000.

CyberSterk
Small and medium-sized enterprises (SMEs) are increasingly aware of the risks posed by cybercrime. Unfortunately, however, many security solutions are too expensive for smaller firms or require too much technical know-how. Even though 99 per cent of Dutch businesses are SMEs. The mismatch represents a growing problem to society. A problem for which we are offering a solution in the form of CyberSterk: a comprehensive package consisting of website and network scans, hardware that detects abnormal internet traffic in a company network, plus good practice tips and tests. Every subscriber gets a weekly automated network and website scan and a report detailing the findings. They also get immediate alerts whenever acute threats are detected. We do regular phishing simulations as well, in which personnel are sent dummy phishing e-mails. However, the service 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.
CyberSterk is made available through the registrar network as far as possible. At the end of December, we had three registrars enrolled as CyberSterk agents.

Outlook

IRMA
In 2020, we'll be working to grow the number of organisations offering IRMA logins to their clients, staff and other users. We're also investigating whether the product should be marketed using an 'as-a-service' model, where we handle everything for the subscriber. Another objective for the year ahead is raising the profile of IRMA amongst end users.

DBS
We're investigating the scope for adding new functionalities to the DBS, such as malicious website content detection. Our analysis will be based on research by SIDN Labs. We've also set ourselves the target of growing the number of subscribers and generating an income of € 315,000.

CyberSterk
By the end of 2020, we want to have around 900 paying subscribers, enrolled through about twenty agents. CyberSterk would then be protecting roughly 20.000 workplaces and websites. With a view to hitting those targets, we're looking to recruit agents from inside and outside the registrar community. Agents will be provided with tooling, demos and other forms of support. We additionally intend to stimulate market demand for CyberSterk by means of targeted campaigns.

In CyberSterk, we are offering a solution to a growing social issue.

"CyberSterk is right up our street."

Eddy Mouws
Managing Director of BusinessConnect B.V.

"As registrars, we get regular newsletters from SIDN. We were interested in CyberSterk as soon as we read about it. A lot of BusinessConnect's customers are SMEs and we place a lot of emphasis on security. So CyberSterk is right up our street. It's a great product! For one thing, it doesn't have any effect on the customer's hardware. All the subscriber has to do is connect a CyberSterk cyber-alarm. Of course there are lots of rival services available to help SMEs protect themselves against cybercrime, but often everything's in English and you need a reasonable level of technical knowledge to make good use of them. By contrast, CyberSterk combines all the features SMEs want in a single product that's easy to understand.

I think it's good that SIDN has launched this product. They're investing in a section of the internet community where online security tends to be neglected. CyberSterk makes it easy for SMEs to start taking security more seriously. This is the first time we've made one of SIDN's extra services available to our customers, and it's been really straightforward. All the material we received from SIDN was very clear. And the support has been good too. That's important, because we have a relatively small team, without a lot of sales expertise. They've been a big help on that front. In fact, when we visited a key prospect, SIDN sent one of their people along to help swing the deal."

17

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

As registry for the .nl domain, we believe we have a duty to serve the local internet community to the best of our ability. We discharge that duty not only by running the .nl zone, but also by enhancing the internet's social and economic value to the Dutch and international internet communities. That involves developing and sharing knowledge, for example, both through our research team SIDN Labs and through other channels. We play an active role in various international forums and collaborate with numerous partner organisations. Through SIDN Fund, we support projects that help to make the internet stronger, promote user empowerment or utilise the internet in innovative ways. Such activities span a wide range of themes, from internet technologies and architectures to standardisation, from internet governance and online citizen rights to digital citizenship.

SIDN Labs

SIDN Labs is our research team: an expertise centre that performs large-scale internet measurements and analyses, develops prototypes, contributes to standardisation and publishes articles, reports and software. By doing so, SIDN Labs helps to improve SIDN's services and to make .nl stronger and the internet 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 and the University of Southern California.

Tackling fake webshops

We have developed FaDe (short for Fake Detector): a new, self-teaching system that automatically identifies fake webshops in the .nl zone by combining machine learning with crawls of the entire zone and the expertise of our Abuse Desk. FaDe is the result of a machine learning strategy devised by SIDN Labs in 2019. It also builds on earlier work in the field of fake webshop detection. Between September and December, the system identified 3,529 suspect domain names. Manual investigations by our Abuse Desk confirmed 2,680 of the suspects as linked to fake webshops. That translates to a detection accuracy of 76 per cent for FaDe. Our abuse experts' conclusions will be fed back into the system, which should enable it to keep learning and improving its predictive capabilities. Working in tandem with the .nl registrars and others, SIDN got 4,340 fake webshops taken down in 2019.

Working in tandem with the .nl registrars and others, SIDN got 4,340 fake webshops taken down.

SPIN

SPIN (Security and Privacy for In-home Networks) is our open-source platform. Its development had two goals: to protect the internet against DDoS attacks mounted by hijacking insecure IoT devices, and to provide users with a better picture of the internet services that the devices on their home networks are communicating with. In 2019, we increased the stability of the SPIN software and made it available as a ready-to-use product that router and modem manufacturers can easily install on their equipment. Although some manufacturers adopted the software, the response from the big players was muted. We therefore decided to put further SPIN product development on hold, while continuing with research use and technical development. In 2019, a paper about SPIN was accepted for the NOMS2020 Experience Session. We also used the intelligence yielded by SPIN to produce a report for ICANN's Security and Stability Advisory Committee (SSAC) describing interaction between the DNS and the IoT.

Research into new types of internet infrastructure

The existing internet's value to the Dutch economy and Dutch society is enormous. It's nevertheless important to consider the potential of new forms of internet, for a variety of reasons. After all, the internet we use today was designed in the 1970s. Its designers couldn't possibly have imagined how we now use it to connect everything from smart grids to drones, and to do everything from remote surgery to cooperative driving. Another problem is that it's increasingly unclear to users what is happening to their data, such as that collected by IoT devices. We're also witnessing a concentration of power over the internet in the hands of big corporations, threatening Dutch and European digital sovereignty. SIDN Labs is 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.

SIDN Labs is studying new types of internet with the potential to complement the existing network.

We started the research in 2019 by looking at SCION, an experimental internet with a testbed and an active community. We connected our own network and developed a beta version of SCION, which supports open programmable switches. We also set up 2STiC, a joint research programme that we're running with the University of Twente, the University of Amsterdam, Delft University of Technology, SURF, NLnet Labs and AMS-IX. A national test network has been established, with open programmable switches, which we plan to extend over the years ahead and use for experimenting with programmable networks, new types of internet infrastructure, new network functions and their applications. We published a blog describing the 2STiC partners' vision for this exciting new field of research and jointly presented a poster at IMC2019.

ENTRADA 2.0

We published version 2.0 of ENTRADA, our open-source platform for analysing large volumes of DNS traffic. The new version enables organisations and researchers to use ENTRADA in the cloud. That lowers the threshold to getting started with ENTRADA, because you don't need to set up your own Hadoop cluster. We ourselves continue to run ENTRADA on our own hardware, mainly because we want .nl's DNS traffic to stay in the Netherlands rather than being stored in the cloud.

Another new feature of ENTRADA is support for the measurement of round-trip times (RTTs) between resolvers and authoritative DNS servers using the TCP protocol.

TimeNL

Time services enable internet-connected devices to synchronise their clocks. Although they are invisible to the average internet user, they are a vital part of the infrastructure, because many different applications depend on precise timing. That's the case with payment transactions, industrial process control, DNS caching, domain name registrations and security mechanisms such as logs and network measurements, to name but a few.

TimeNL is a public time service that we developed on the basis of the NTP (Network Time Protocol). We were motivated by the discovery that many public time services disclose little information about service levels (accuracy, maintenance, etc) and rely exclusively on GPS. By contrast, TimeNL is transparent about its service level and makes use of three mutually independent time sources (GPS, Galileo and DCF077). We've also added support for NTS (Network Time Security), the security extension to NTP.

DDoS clearing house

Back in 2018, we teamed up with the University of Twente and SURF to propose the creation of a national DDoS clearing house: a system for the continuous automated exchange of 'DDoS fingerprints' amongst service providers. Each fingerprint is a statement of the characteristics of a DDoS attack that the compiler has dealt with, which others can use to proactively prepare their own infrastructures to ward off a similar attack.

The DDoS clearing house initiative has ten participants, including KPN, NBIP-NaWas, VodafoneZiggo, the Dutch Payments Association and SURF. In 2019, we worked with the other members to draft a fingerprint sharing agreement and build a prototype clearing house. Through the CONCORDIA project, we also contributed to the creation of a European DDoS clearing house.

DNS measurements

Along with the University of Twente, NLnet Labs, the USC/Information Sciences Institute, Verisign and the Rochester Institute of Technology, we undertook a longitudinal study to follow up the DNS root KSK rollover of 11 October 2018. The results were described in a paper that was accepted for presentation at the internationally prestigious ACM Internet Measurement Conference (IMC2019), where it won a Distinguished Paper Award.

We also investigated the use of DNS TTL values and used the findings to formulate a set of recommendations, which have since been adopted by our own DNS operations team and three other ccTLDs (including Uruguay's). The recommendations were additionally included in a best practice document for authoritative DNS operators, which is currently under review within the IETF. The research was done in collaboration with experts at the USC/Information Sciences Institute and the University of Passo Fundo. A paper describing this project too was presented at IMC2019, as was a third paper on DNS resolver measurements.

Other measurement studies performed in 2019 looked at the use of QNAME minimisation and the classification of resolvers that query the .nl name servers.

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 235 innovative projects.

The Fund's first call for proposals of 2019 followed the established open model. A new approach was adopted midway through the year, however. With a view to maximising impact, the Fund decided to focus future calls on selected priority topics. That led to two themed calls: 'Public values in the digital society' and 'Keeping control of your data'. SIDN Fund also committed to more intensive collaboration with relevant partners. On the 'Public values in the digital society' call, for example, the Fund worked closely with the Adessium Foundation. Another innovation in 2019 was the switch to accepting Pioneer Project proposals all year round, rather than

only during defined time windows. Pioneer Projects are smaller projects requiring grants of up to €10,000. Following careful consideration by the Fund's staff and Advisory Panel, grants were awarded to a total of 51 projects in 2019.

The year also saw SIDN Fund become a theme partner to the National ThinkTank, an annual project for tackling social problems. Each year, a fresh ThinkTank is assembled by selecting young, motivated academics: doctoral students, master's students and recent graduates from various backgrounds and with various forms of work experience. The group then spend four months getting to grips with an issue. In 2019, the ThinkTank was asked to address the social challenges posed by digitisation.

In November, SIDN Fund linked up with Google, Brinkhof Advocaten and Greenhost to organise the Internet Thesis Awards.

"We couldn't have done this without support from SIDN Fund."

Wido Potters
Treasurer of the AbuseIO Foundation

22

"The AbuseIO Foundation produces open-source software for fighting abuse. Our volunteer engineers have developed two distinct software packages. One is designed to help hosting service providers systematically process abuse reports received from a variety of sources. The other is specifically for use by the Reporting Hotline for Internet Child Pornography. It enables the Hotline to quickly and efficiently refer child pornography reports to hosting firms. That's very important, because they get about half a million reports a year, all of which need to be analysed by the charity's staff. If the analyser decides that a reported item is child pornography, they have to find out who hosts the site, look up the firm's abuse contact details, and send an e-mail. And, until recently, that all had to be done manually. But our software now handles those administrative tasks.

Building the Hotline's software was quite an undertaking. If we'd had to rely on our volunteers to do everything, it would have taken years. However, we were able to hire temporary programmers, so that the work could be done more quickly. We couldn't have done that without support from SIDN Fund. I knew about the Fund from SIDN's newsletters. So I got in touch, and they were really helpful. They provided a lot of very clear guidance, enabling me to put together a persuasive proposal. Later on, I was also able to attend various information sessions organised by the Fund, including one about open-source software licences. As well as getting loads of help, I learned a lot too."

Some of the projects supported by SIDN Fund

Web archivering XS4ALL homepages

XS4ALL is one of the oldest internet access providers in the Netherlands. Many internet pioneers used the firm's services to build their first homepages. Dating from the infancy of the Dutch web (1993-2000), the sites represent an important part of our digital heritage. The Dutch National Library therefore set up a project to preserve as many of the homepages as possible.

AmberScript

The Netherlands is home to more than 1.3 million people who are deaf or hard of hearing. Without an interpreter, it's very hard for them to spontaneously strike up a conversation or get to know new people. AmberScript is therefore developing a Dutch-language speech recognition app that will convert speech to text in real-time. People with hearing problems will be able to use the app free of charge.

Continuous Accessibility Checker

People with impaired vision want to be able to use the internet like everyone else. However, many online services aren't designed with such people in mind. This project therefore involves development of a tool for checking during the test phase how accessible new software is for people with impaired vision. The tool will enable software developers to spot accessibility problems at an early stage.

Privacy Label

Privacy statements on websites and elsewhere explain what will happen to your personal data. However, many consumers don't read privacy statements, or don't fully understand them. Privacy Label aims to address that by making privacy statements clearer and more accessible. Icons and simplified explanations will provide information about personal data processing within an organisation.

Trends in Online Security & e-Identity

In 2019, we extended our annual trends survey by studying trends in e-identities and cybersecurity. In partnership with Connectis, more than two thousand consumers and 500-plus business decision-makers were surveyed.

A shocking 90 per cent of Dutch businesses don't see cybercrime as a (serious) threat to their activities.

The findings revealed that the Dutch business community is dangerously relaxed about cybercrime. A shocking 90 per cent of businesses don't see it as a (serious) threat to their activities. Indeed, 17.6 per cent of them said it wasn't a threat at all. Willingness to invest in security is correspondingly low: a significant majority (69.4 per cent) of businesses expect no change in spending on security in the year ahead. For larger organisations, the main concerns

are DDoS attacks and the theft of intellectual property and customer data. Smaller organisations rated malware as the biggest threat. It was partly in light of those findings that we decided to develop CyberSterk, a service designed to help SMEs protect themselves against malware, phishing and other threats.

More than half (57.2 per cent) of consumers say that they use social log-ins, such as Google and Facebook, on a daily basis. Yet only 14.4 per cent say that they think such behaviour is safe. Similarly, 54.4 per cent use a user name-password combination every day, although only 37.5 per cent see that as a secure way of logging in. Consumers are lax about protecting their online identities as well. Just 22.7 per cent of respondents use a strong password, and even fewer opt for multi-factor authentication. What consumers worry about most are identity fraud, hacking and personal data theft.

SIDN Panel

In order to keep improving our services, we want to get the views of businesspeople. In 2019, we therefore set up the SIDN Panel: a fixed group of respondents who give us regular feedback. Among the topics we asked them about were business e-mail use, online security and the trustworthiness of domain names.

Internet security awareness

We helped to raise internet security awareness through our newsletter and numerous articles on our website.

Sharing knowledge with registrars

Two webinars were organised to share knowledge with registrars and hosting firms. The first was about our plans for the .nl zone, while the second was devoted to the DANE e-mail security standard. Developed in association with the RA, the webinars were followed by 120 registrars.

Courses and workshops were made available to registrars through our SIDN Academy. In 2019, we teamed up with the Registrars' Association to organise a successful second Academy session. The session focused on IPv6 implementation for registrars and hosters, with the aim of increasing knowledge and promoting adoption. We ran the session three times, attracting a total of seventy-five participants. Asked to rate the SIDN Academy, people who attended gave it eight out of ten.
The impact of our knowledge-sharing activities was reflected in significant growth in the number of .nl domain names with secure mail servers.

SIDN TechTalk

Under the SIDN TechTalk banner, we organised three successful meetings at our offices. The events were intended for technicians and students in the surrounding region. The events were used to share knowledge gained through collaboration with universities and colleges, (international) tech companies, and working groups on abuse and data security. Topics addressed included abuse control, IPv6 and the DNS. The three SIDN TechTalks were well received by the average of forty people attending, who gave a satisfaction score of 8.4 out of ten.

*SIDN TechTalk attendees gave a satisfaction score of 8.4 out of ten.*

Cybercrime Prevention Covenant

In September, we put our name to the Cybercrime Prevention Covenant. The move aligned us with signatories including the Ministry of Justice and Security, the Ministry of Economic Affairs and Climate Policy, several representative organisations and various important companies. The Covenant provides for concerted action to promote internet crime prevention measures.

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.

Fig. 8 | DANE
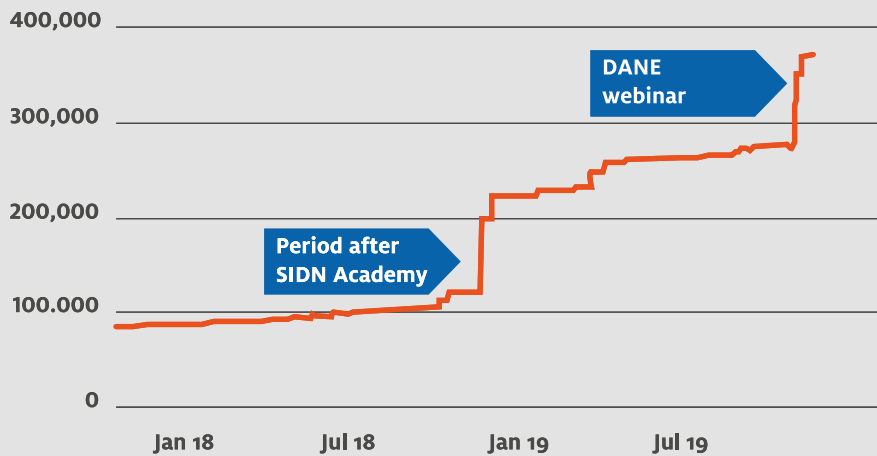
Contributions to organisations and conferences

We play an active role in various important international forums. In 2019, we again participated in numerous national and international meetings, helping to organise several of them.

ICANN

ICANN meetings were held in Kobe (9-14 March), Marrakesh (24-27 June) and Montreal (2-7 November). Stakeholders from all around the world gathered to address policy issues, particularly concerning the Domain Name System. Ahead of each meeting, we worked with the Ministry of Economic Affairs and Climate Policy to organise preparatory sessions for Dutch people intending to go to the ICANN events. Within ICANN, we sit on the ccNSO SOP Committee and the SSAC. We also represent the ccNSO at the GNSO Council and within the IANA IPR Community Coordination Group.

As well as attending the three meetings, we were at the ICANN GDD Industry Summit in Bangkok (6-9 May).

RIPE

We have been working with RIPE for many years. We participated in both the RIPE meetings held in 2019, in Reykjavik (20–24 May) and Rotterdam (14–18 October). SIDN Labs spoke about the findings of our research into the DNSSEC root KSK rollover's impact on the DNS, and into optimum time-to-live (TTL) settings in the DNS.

IETF/IRTF

We attended the IETF meetings in Prague (23-29 March), Montreal (20-26 July) and Singapore (16-22 November). At the meetings, we were active contributors. Along with the University of Southern California/Information Sciences Institute, for example, we submitted an Internet Draft for authoritative DNS operators, based on research by SIDN Labs.

CENTR

CENTR – the umbrella organisation for European ccTLDs – marked its twentieth anniversary in 2019. We were one of the foundation's first members. CENTR organises various gatherings, at which members exchange experiences and discuss developments. One of CENTR's events is an annual Registrar Day, which we invite .nl registrars to attend with us. In 2019, we also had the privilege of

hosting the CENTR Jamboree, from 27 to 29 May in Amsterdam.

At the CENTR Awards Ceremony in Brussels on 8 October, we received no fewer than 4 prizes.

At the CENTR Awards Ceremony in Brussels on 8 October, we received no fewer than four prizes. We took the Innovation Award for developing a model that provides registries with a clear picture of their security status, relative to a range of defined benchmarks. Our second accolade was a Member Award in recognition of all our input and contributions. Finally, our Marketing Manager and our Legal and Policy Manager both picked up Working Group Champion Awards for their personal contributions to the CENTR community.

25

ECP Annual Congress

We were once again pleased to support the ECP Annual Congress, held on 14 November. The event's theme was The Future of the Information Society. Our input included making and showing a short video, in which Erik Huizer, Frances Brazier, Kees Neggers, Ted Lindgreen, Jaap Akkerhuis and Boudewijn Nederkoorn reflected on fifty years of the internet. All were amongst the internet pioneers who connected the Netherlands to the world. We also organised four workshops on The Internet of the Future. One involved a discussion with Marleen Stikker, Kees Neggers, Michiel Steltman and Valerie Frissen, CEO of SIDN Fund. Several of the projects supported by the Fund gave demonstrations, while SIDN Labs presented its work on SCION, an experimental future internet.

NL IGF

In 2019, the NL IGF event was incorporated into the ECP Annual Congress. NL IGF is a preparatory national event held ahead of the international Internet Governance Forum, the United Nations' multistakeholder platform. Input gathered at the NL IGF was presented to the international IGF in Berlin. At NL IGF, SIDN Labs linked up with KPN to make a presentation on DNS-over-HTTPS.

Internet Governance Forum

We were part of the Dutch delegation at the Internet Governance Forum in Berlin. At the event, we lent our support to efforts to accelerate the adoption of internet standards.

EuroDIG

We're among the organisations that support EuroDIG, the European Dialogue on Internet Governance. In that role, we joined ECP and the Municipality of The Hague to host EuroDIG 2019 in The Hague. 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. 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 Labs facilitated a session on centralisation of the internet.

IDnext '19

Since 2015, we've partnered IDnext, an open, independent platform that supports innovative developments in the field of digital identities. In 2019, we broadened our involvement by helping to organise IDnext '19, held in The Hague on 25 and 26 September. IDnext is Europe's leading independent, interdisciplinary conference for experts and key players in the world of digital identification.

One Conference 2019

From 1 to 3 October, enterprises, governments and academics from all over the world met in The Hague to share cybersecurity knowledge and experiences. SIDN Labs and its research partners made three presentations at the conference.

The Internet Measurement Conference

We sponsored and helped to organise the ACM Internet Measurement Conference 2019, a major event with a global profile held in Amsterdam from 21 to 23 October. The conference brings together leading academics and industry representatives to discuss internet measurement issues. Together with its research partners, SIDN Labs succeeded in getting no fewer than three papers accepted for presentation at the conference. To be accepted, a paper has to undergo rigorous review by independent experts. Our analysis of the first ever DNSSEC root KSK rollover was recognised with a Distinguished Paper Award.

SIDN Labs succeeded in getting no fewer than three papers accepted for ACM Conference.

SIDN Connect

On 28 November, we held the third edition of our SIDN Connect event, bringing together partners of SIDN, SIDN Labs, Connectis and SIDN Fund for a day on the KNVB Campus in Zeist. Attendees enjoyed a range of inspiring talks and thought-provoking sessions.

Partnerships and sponsorship

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.

Internet Security Platform

The Internet Security Platform is a joint public-private initiative intended to promote internet security. In 2019, we were again active participants, with representation on the steering committee of the popular site Internet.nl, for example.

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

The Online Child Abuse Expertise Bureau developed from the Reporting Hotline for Internet Child Pornography. Its mission is fighting the distribution of child sex abuse images on the internet.

Alert Online

Alert Online is an annual 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.

Bits of Freedom

In 2019, we extended our sponsorship of Bits of Freedom, a foundation that defends freedom and privacy on the internet. Freedom and privacy are fundamental rights, and essential for development, technological innovation and the rule of law. Bits of Freedom fights for an internet that is open for everyone, where private communication remains private.

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 supply the facilities on which the digital economy is based – data centres, hosting service providers, internet service providers and others. We were one of the organisation's founders.

ECP (Electronic Commerce Platform)

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.

ISOC.nl

The Internet Society has 44,000 members in 170 different countries. It is the parent organisation for various international bodies, including the IETF, IAB and IRTF. In the Netherlands, ISOC.nl has about a thousand members from the internet industry, business and government.

NLnet Labs

NLnet Labs is a Dutch R&D institute with a strong international reputation. We are a major co-funder of NLnet Labs' work, and SIDN Labs often undertakes projects with the institute on a collaborative basis. Cristian Hesselman, Director of SIDN Labs, chairs the NLnet Labs Board.

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.

27

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. We support ISPConnect because we believe that it's important for the ISP sector to have an effective advocate.

Outlook

SIDN Labs

Data sharing

In 2020, our research team will continue using its findings to support service enhancements, by developing tools for our Abuse Desk and our DNS operations team, for example. Aggregated data gathered using such tools will be published on stats.sidnlabs.nl, shedding light on matters such as fake webshop detections within a given time window. We will also continue publishing our research results in the form of papers and presentations. The ultimate goal of our measurement and analysis projects is to enable us to become an authoritative news outlet for the internet.

An ENTRADA for the Internet of Things

SIDN Labs is looking at the possibility of building a research platform like ENTRADA, but for processing data on the network traffic associated with IoT devices. Potential data sources include SPIN and server-side systems, such as IoT honeypots. Our aim is to make the datasets available to the Dutch research community.

2STiC

Within the 2STiC research programme, we are developing a demo of a sector-specific application on the national 2STiC testbed. The application will shed light on the added value of new internet architectures such as SCION and RINA, and is expected to tell us a lot about their implementation on open programmable routers.

DDoS clearing house

In the year ahead, we intend to extend the Dutch DDoS clearing house pilot. The pilot is providing input for the European CONCORDIA project, which is intended to yield a blueprint for the creation of clearing houses in other countries.

SIDN Fund

While project support will remain SIDN Fund's core task, the way that deserving projects are identified is changing. As well as organising open calls for proposals, the Fund intends to place more emphasis on themed calls and scouting. SIDN Fund is also committed to more intensive collaboration with relevant partners.

SIDN Academy

In partnership with the RA, we are creating an online branch of the SIDN Academy, where stakeholders can boost their expertise on a range of technical subjects. The platform will make integrated use of online and offline teaching methods. The first e-learning module, devoted to e-mail standards, was made available at the start of 2020. Later this year, we'll be adding modules on the DNS, DNSSEC and IPv6.

28

"Where do the time checks used by computer systems actually come from?"

Marco Davids
Research Engineer at SIDN Labs

"As a registry, SIDN works with the Domain Name System (DNS). Although it's one of the key technologies supporting the internet, the DNS goes largely unnoticed: every internet user uses it all the time, without really realising. In 2019, I started to take a closer interest in another fascinating 'hidden' technology: NTP, the Network Time Protocol. Again, it's something we all use constantly without knowing it.

As the name suggests, the NTP is all about time. Time plays a big part in our daily lives. There are countless situations where it's important to know whether one event happened before another, or after. Situations where we need to know when an event occurred, or what the interval was between two events. In many cases, precision is vital. Time is important in computing too. Computers therefore have built-in clocks, which many applications refer to, and some depend on. The NTP was developed to keep those internal system clocks synchronised. It allows for computer clocks to be set extremely precisely via the network.

However, the more you explore the NTP landscape, the more aware you become of the lack of transparency. Where do the time checks used by computer systems actually come from? How reliable are they? And how do you contact the people who run the time services? Answers to questions like that are often difficult – if not impossible – to come by. Another issue is that many NTP services rely exclusively on the US GPS system as their reference source. So, here in Europe, we're dependent on the US to a degree. With all that in mind, we decided to start our own public NTP service. TimeNL is completely transparent about how it works and how it's managed. And, instead of relying entirely on GPS, we use Europe's Galileo signal as a time source. Our service is free for anyone to use, and it has its own website, packed with useful information. Another plus, of course, is that the service is delivered by SIDN, a trustworthy non-commercial provider committed to quality and security."

> Read more about TimeNL

04

Real social impact

Internal developments

Real social impact
Internal developments

SIDN is an organisation with considerable social impact. We manage nearly six million .nl domain names and the infrastructure that enables those names to be used at any given moment. We play a key role in various international consultation forums, undertake research, develop new products and collaborate with numerous partner organisations. Within the company, there is a strong sense that we are working for the good of the nation and the wider world.

We are a true knowledge-based organisation with a highly trained, expert workforce. 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.

We worked hard to enhance our position on the labour market in 2019.

Workforce
Like many organisations, we face the challenge of operating in a very tight labour market. Our HR and Communications Departments therefore worked hard to enhance our position on the labour market in 2019. We upgraded our 'Working at SIDN' site, for example, modified various communication tools and added a recruiter to the payroll. We also developed a network, optimised our collaboration with universities and colleges, and increased the number of internships available to students and others. Other focus areas included our recruitment process and the way we settle in new recruits. Our efforts on the various fronts were rewarded: by the end of the year,

we had filled twenty of the twenty-five vacancies we had at the start, most of them in challenging technical fields, such as ICT. As a result, we ended the year with a workforce of 110 (102 FTEs). Of those, 35 per cent were women and 65 per cent men.

Agile working
Agile working was introduced in 2017, with a view to increasing our ability to respond to dynamic situations and reducing time to market. In 2019, we shifted significant decision-making authority to lower levels of the organisation and increased the use of multidisciplinary, self-managing teams. We also adjusted our performance management arrangements and our remuneration structure.

Changes to our organizational structure
We transferred our new activities, including CyberSterk and IRMA, to a new legal entity, SIDN Business B.V. The move means that any risks arising from such activities cannot have a negative effect on our core role, management of the .nl zone.

Meanwhile, our management team was superseded by an executive team. The aim being to allow our various units to operate on a more independent basis. The executive team was additionally strengthened by the appointment of a Chief Financial Officer, Tuyen Nguyen. Tuyen has responsibility for the financial strategy of SIDN group as a whole (SIDN, SIDN Labs and Connectis), and for underwriting SIDN Fund.

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. In 2019, greater use was made of one-to-one coaching, which is promoted through our new performance management mechanism.

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. The scheme is actively used to assist sport clubs, musical societies, charities and all sorts 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 2011, we became the first registry in the world to achieve ISO27001 certification. The 2019 audit found no issues of concern, and our certificate was renewed for the ninth time.

Staff Council

In 2019, several proposals were referred to the Staff Council for approval, in connection with matters such as the introduction of Agile Performance Management as an alternative to the traditional appraisal system. The Council was also involved with development of a new privacy policy. In addition, the Council was kept informed regarding SIDN's annual plan and budget for 2019. A meeting between the Council and SIDN's Supervisory Board took place in June.

Outlook

Staff Survey

In the early part of 2020, we will undertake a survey to gauge the satisfaction, engagement and motivation of our workforce.

Team development

We attach great importance to a strong team ethic. Teamworking is promoted in a variety of ways, including workshops and training sessions devoted specifically to topics such as team effectiveness and coaching leadership.

Tight labour market

Recruitment remains challenging, particularly where IT roles are concerned. Energetic efforts to increase our profile and boost our image as an employer will therefore continue in 2020. Particular emphasis will be placed on onboarding, campus recruitment and more active use of social media.

"It's important to know whether things are genuinely secure, or just seem to be."

Erwin Janssen
Student intern at SIDN Labs

"A lot of internet traffic is secured using Transport Layer Security (TLS) – the protocol behind the familiar green padlock you see when you visit a website that supports HTTPS. Programs that want to use TLS need to utilise software libraries. Over time, however, various vulnerabilities have been discovered in the libraries, prompting the release of new versions. To be secure, therefore, programs really have to be using the latest software library versions. The question is, are they?

For my dissertation study, I've developed a tool that sends a series of messages to a TLS server in order to find out which version of which software library it's using. You then know whether it's up to date or vulnerable. My tool can be used to do mass surveys of internet servers to find out whether they're using a secure version of TLS. That's useful, because it's important to know whether things are genuinely secure, or just seem to be."

05
Report by the Supervisory Board

Diversification

SIDN well prepared for the period ahead

The Supervisory Board maintains general oversight of SIDN and its Chief Executive, providing support and 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. One issue to occupy the Board in 2019 was SIDN's new organisational structure.

Meetings

The Supervisory Board met four times in 2019, and also had one discussion with the Registrars' Association. The SB additionally met SIDN's Staff Council in June. There was regular contact with SIDN's CEO between meetings. Particular attention was given to the organisational changes. The Supervisory Board's various committees additionally met a number of times.

- Audit Committee: two meetings
- Selection and Appointments Committee: no meetings
- Security and Stability Committee: two meetings

The following were approved and/or adopted:

- SIDN's Annual Report and Annual Financial Statement for 2018
- 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 2020
- Incorporation of SIDN Business B.V. as a separate entity to undertake new business activities, such as IRMA and CyberSterk (all shares held by SIDN)
- Proposals regarding decisions to be taken by SIDN in its capacity as shareholder in SIDN Deelnemingen B.V., e.g.:
  - Adoption of the Annual Financial Statement of SIDN Deelnemingen B.V. for 2018
  - Approval for adoption of the Annual Financial Statement of Connectis Group N.V. for 2018
  - Approval for adoption of the annual plan and budget of Connectis Group N.V. for 2020

Membership

The Supervisory Board has seven members. Its membership did not change in 2019.

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

Conclusions

The Supervisory Board believes that the policies pursued by SIDN have been such that the quality of SIDN's services is assured and that the company is ready for the immediate future. The quality of SIDN's infrastructure is high. The company has a very competent workforce and continues to recruit capable personnel, despite the tight labour market conditions. SIDN's new organisational structure is expected to enhance operational quality, security and agility. The .nl domain grew slightly in 2019 and the organisation is in good financial health. SIDN Fund has proved very successful and substantial sums are being invested in new products and services. Satisfaction with SIDN's services remained high amongst registrars in 2019, and SIDN works closely with its registrars in many fields. It is therefore regrettable that differences of opinion persist between the Registrars' Association and SIDN regarding some of the latter's strategic decisions. The Supervisory Board nevertheless adheres to the view that diversification through initiatives such as CyberSterk is extremely important in terms of enabling SIDN to remain of value to the local and wider internet communities in the long term.

36

Paul Schnabel,
Chair of the Supervisory Board

06

Financial statement

Notes to the Annual Financial Statement

In line with our annual plan, the net result for the 2019 financial year was a negative sum of €3.7 million (2018: €4.0 million negative). The result is an extension of our stated financial policy of making effective use of a proportion of our accumulated reserves. That includes making donations to SIDN Fund, increasing spending on SIDN Labs, operating an incentive scheme for .nl registrars (the Registrar Scorecard), and funding projects that contribute to the improvement of .nl and have direct commercial benefit for registrars ('registrar projects').

The operating result, excluding donations to SIDN Fund, was a negative sum of €1.3 million. That is €0.5 million down on 2018 (€0.8 million negative), due to a fall in net turnover.
In 2019, the number of registered domain names increased slightly, but turnover fell slightly relative to 2018, mainly as a consequence of a one-off correction to previously reported figures. The correction related to the attribution of turnover in previous years. Operating costs remained at the same level as in 2018, namely €22.8 million. Personnel costs for the year were €10.3 million and accounted for roughly 45 per cent of the total costs (2018: 43 per cent). That represents a rise of 3.8 per cent relative to the previous year (2018: €9.9 million). Numerous vacancies were filled in 2019, resulting in less use of external staff. The lower expenditure on external staff offset the rise in social security and pension contributions. Salaries rose as a result of index-linked adjustments and the organisational changes made. The other operating expenses remained stable and the lower depreciation changes in 2019 were at a normal level.

The settlement agreed with the tax authority regarding the status of the donations to SIDN Fund led to a one-off fiscal charge in the 2018 financial year. The corporation tax payment in 2019 reflected the agreement, resulting in an effective taxation charge of -5 per cent.

Our share in the net result of Connectis Group B.V. ('Connectis') for 2019 was a negative sum of €0.3 million. In 2019, Connectis continued to invest in scaling up services and products, and met its financial targets for 2019.

The cash flow in 2019 was a negative sum of €0.8 million, attributable mainly to investments in hardware and equipment.

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 liquidity of between 65 and 100 per cent of the structural cost base. At the close of 2019, both solvency and liquidity 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.

Outlook

In recent years, we have made effective use of a proportion of our accumulated reserves by increasing investment in the internet community, registrar projects and incentive schemes. Having reduced our capital and reserves to an appropriate level, we intend to reduce investment and expenditure in the coming years to a level commensurate with the prevailing circumstances.
At the end of 2019, the new IRMA and CyberSterk services were introduced to the market. Income from both services is expected to increase substantially in the years ahead. Personnel costs will increase slightly as a result of the development of the new services. Investment is expected to remain unchanged. The net effect is expected to be an uplift in our operating results, relative to 2019.

In March 2020, SIDN Deelnemingen B.V. decided to sell all its shares in Connectis Group B.V. to a third party. The decision was subsequently endorsed by SIDN (the shareholder) and by SIDN's Supervisory Board. The contract governing the sale was finalised and signed in early March 2020. It is expected that the transaction will be completed during 2020. Through the sale, SIDN Deelnemingen B.V. will more than recover the price paid to acquire the shareholding. Furthermore, under the terms of the sale, SIDN Deelnemingen B.V. will acquire an interest in a new company, of which Connectis will become part. Additional information is provided in the Notes to the Annual Financial Statement.

Another major event has taken place since the balance sheet date, namely the COVID-19 outbreak. When the outbreak began, we acted promptly in anticipation of the government's restrictions. We have prioritised the continuity of our services and the health of our staff. Both are adequately assured by our IT systems, which provide full support for working from home. We continue to monitor developments closely and will take further action if necessary or desirable.

Risks and uncertainties

Vision and policy

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

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 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.

Before starting a project, we produce a project plan, which always includes a section covering the risks associated with the project, the risk management measures to be taken and residual risks. Before the project is given the go-ahead, consideration is given to the risk section of the project plan. Any changes to the risk situation and the risk management measures are addressed in the regular project progress reports.

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.

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. We do not have a direct sales channel to the end market and therefore have very little scope for influencing that market ourselves. The focus is consequently on collaboration with our registrars, e.g. through the Registrar Scorecard, which offers incentives to promote the adoption of IPv6, DNSSEC and the use of e-mail security standards. At the same time, we are seeking to increase our added value, extend the range of services we offer and thus reduce our dependence on .nl.
We have accordingly added a second component to our strategy: maximising impact through growth in the e-identity and cybersecurity domains. At the start of 2017, we gave expression to that strategy by acquiring a 65 per cent interest in Connectis. The acquisition was made through SIDN Deelnemingen B.V., a wholly owned SIDN subsidiary. That was followed in 2019 by the preparation of two new products -- IRMA and CyberSterk -- for market introduction.
Our strategic risk appetite is moderate in relation to activities with the potential to increase our added value..

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.

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 Whois/Is, the power supply, our office IT 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 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 breaches of the confidentiality or integrity of important data. Our risk appetite in relation to activities with the potential to increase operational excellence is moderate.

Financial risks
- Damage claims and penalties: service interruptions and data confidentiality or integrity breaches have the potential to generate claims and/or penalties. Our General Terms and Conditions limit or exclude our liability for such problems.
- Currency/exchange rate risk: our exposure to currency and exchange rate risks is modest. Our .nl services are priced in euros and we make little use of suppliers that charge us in other currencies.
- Bad debt risk: 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.
- Liquidity risk: our liquid assets are divided across three Dutch banks. In 2017, we acquired a portfolio of Dutch and German government bonds.
- Market risk: 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.
- Solvency risk: we maintain a financial buffer to assure the continuity of the organisation (for a period) in the event of a significant loss of our earnings and/or the need for high expenditure at short notice. The minimum size of the buffer increases in step with our structural cost base. The financial

buffer is currently above the defined minimum.
- Uncertainty about our ability to attract finance: to date, we have not needed to seek external finance.

Our financial risk appetite is 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 required to inform the NCSC and the regulator of any serious incident 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 2019. 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.

Consolidated financial statements for 2019
Consolidated balance sheet as at 31 December 2019 (after appropriation of profit)

Fixed assets	31 December 2019 (in €)	31 December 2018 (in €)
Intangible fixed assets	6,021,677	6,992,515
Tangible fixed assets		
Land and buildings	4,968,951	5,147,068
Machinery and equipment	816,494	836,742
Other fixed business assets	574,703	608,821
Tangible fixed assets under development	47,054	29,174
	6,407,202	6,621,805
Financial fixed assets	3,999,271	3,790,524
Current assets		
Receivables		
Trade receivables	207,694	296,789
Tax and social security contributions	383,948	1,208,846
Other receivables and accrued and deferred assets	948,738	1,211,978
	1,540,380	2,717,613
Liquid assets	17,577,002	18,384,811
	35,545,532	**38,507,268**

Passiva

	31 December 2019 (in €)	31 December 2018 (in €)
Long-term liabilities	24,280,705	28,149,021
Long-term liabilities		
Other liabilities	442,651	406,250
Short-term liabilities		
Accounts payable	732,932	1,104,879
Tax and social security contributions	480,480	420,679
Other liabilities and accrued and deferred liabilities	9,608,764	8,426,439
	10,822,176	9,951,997
	35,545,532	**38,507,268**

42

Consolidated profit and loss account for 2019

	2019 (in €)	2018 (in €)
Net turnover	18,934,295	19,481,759
Expenditure		
Wages and salaries	7,338,005	7,345,103
Social liabilities	844,949	709,964
Pension costs	1,167,679	978,649
Other personnel costs	980,136	916,093
Depreciation	1,821,568	2,518,557
Other operating expenses	10,596,751	10,518,465
	22,749,088	22,986,831
Operating result	-3,814,793	-3,505,072
Financial income and expenditure	41,327	48,067
Result before taxation	-3,773,466	-3,457,005
Taxes	180,584	-726,371
	-3,592,882	-4,183,376
Result from participating interests	-275,434	200,557
Result after taxation	**-3,868,316**	**-3,982,819**

43

Consolidated cash flow statement for 2019

	2019 (in €)	2018 (in €)
Cash flow from operating activities		
Operating result	-3,814,793	-3,505,072
Adjustment for:		
Depreciation	1,739,593	2,518,557
Movement in provisions	201,462	-
	1,941,055	2,518,557
Movement in working capital:		
Movement in receivables	-263,306	-253,002
Movement in short-term liabilities	870,179	665,339
	606,873	412,337
Cash flow from operating activities	-1,266,865	-574,178
Interest received	19,283	1,145
Corporation tax	855,925	-587,155
	875,208	-586,010
Cash flow from operating activities	**-391,657**	**-1,160,188**
Cash flow from investment activities		
Investments in intangible fixed assets	-	-268,099
Divestment of intangible fixed assets	6,336	-
Investments in tangible fixed assets	-636,556	-247,493
Divestment of tangible fixed assets	76,068	-
Movement in other financial fixed assets	-	-266,133
Income from securities	138,000	-
Cash flow from investment activities	-416,152	-781,725
Increase / (decrease) in funds	**-807,809**	**-1,941,913**

44

Consolidated cash flow statement for 2019

	2019 (in € 1,000)	208 (in € 1,000)
Analysis of funds		
Funds as at 1 January	18,384,811	20,326,724
Movement in liquid funds	-807,809	-1,941,913
Funds as at 31 December	**17,577,002**	**18,384,811**

07

Directors and officers

Directors and officers as of 31 December 2019

Chief Executive Officer

Roelof Meijer

Supervisory Board

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

Executive Board

Cristian Hesselman, *Director of SIDN Labs*
Arjan Middelkoop, *Commercial Director*
Tuyen Nguyen, *Chief Financial Officer from 1 May*
Cees Toet, *Operational Director*

Staff Council

Sebastiaan Assink, *Chair until 1 December 2019*
Barry Peters, *temporary Chair from 1 December 2019*
Remko van den Berg
Martin Sluijter, *Secretary*
Ruben Wubbels

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.

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.

General Data Protection Regulation (GDPR)
From 25 May 2018, uniform privacy legislation will apply throughout the EU: the General Data Protection Regulation (GDPR).

Big data
A very large volume of digital information gathered for analysis, often from various sources.

Blockchain
The technology underpinning many cryptocurrencies, including Bitcoin. In principle, it works like a general accounting ledger.
However, it isn't maintained by a central administrator, but by all its users. When one user performs a transaction, it is immediately recorded by all users. Its decentralised structure makes a blockchain unhackable.

Caching
Storing data in temporary files. Retaining frequently visited web pages in a cache means that the same information doesn't have to be fetched repeatedly.

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.

Cloud computing
Computer services, such as storage, database management, networking and software, which are delivered via the internet ('the cloud'). Examples include video streaming and online gaming.
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.

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.

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.

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

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.

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

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.

49

General Data Protection Regulation (GDPR)
From 25 May 2018, uniform privacy legislation will apply throughout the EU. The Dutch regulation implementing the GDPR is the Algemene Verordening Gegevensbescherming (AVG).

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.

E-invoicing
The electronic exchange of invoices.

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.

Fake webshop
An internet site that looks like a normal webshop, but actually exists only to defraud visitors.

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.

Identity and access management (IAM)
The collective processes by which an organisation administers and manages network users, including for example processes for managing access to applications and systems.

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 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
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 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.

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.

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.

ISOC (Internet Society)
An international organisation for worldwide collaboration and coordination on matters relating to the internet and the associated technologies and applications. ISOC brings together sixteen thousand internet professionals in 180 countries, many of whom helped to create the internet.
See also internetsociety.org.

Internet Society of the Netherlands (ISOC.nl)
A society of about eight hundred members from backgrounds including the internet industry, the business community, government, consumers' organisations, the non-profit sector, the technology industry and the financial, legal and academic domains.
See also isoc.nl.

Java
A programming language that is widely used on the internet.

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.

New gTLD Programme
An ICANN initiative: the largest extension to the domain name system ever. In 2013, the number of generic domain names was increased from twenty-two to more than a thousand.

50

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.

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.

Real time
The actual amount of time required to do something. Real-time interaction is interaction without delays or data processing waiting periods.

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.

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.

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.

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'.

Internet service provider (ISP)
A business that provides internet services, e.g. online TV and internet telephony. ISPs typically also provide network equipment for home networks.

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.

Single sign-on
Single sign-on-software enables a network user to gain automatic access to multiple applications or resources by signing on once. It therefore removes the need to enter a password repeatedly.

Spam
Unsolicited e-mail.

SSL
A data encryption technology for securing the connection between a website visitor and the website's server.

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.

Unicast
A way of exchanging data on a computer network, where data packages go from a single source to a single destination (host).

Uptime
The period that a computer system or network is available.

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.

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.

51

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.

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

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

52

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, Verenigd Koninkrijk

© SIDN

Text and figures from this report may be reproduced, but we ask that you let us know of your intentions in advance by mailing communicatie@sidn.nl and that you credit us as the source.

Subscribe to our newsletter

www.sidn.nl/nieuwsbrief