

2021

Annual Report

35 years .nl - 25 years SIDN



For confidence online

2021

Contents

	<u>Foreword: Why a strong internet matters</u>	2
01	<u>A .nl domain that delivers value and embodies values</u>	7
02	<u>Impact in two domains</u>	18
03	<u>Profit with a purpose</u>	23
04	<u>Internal developments</u>	38
05	<u>Report of the Supervisory Board</u>	44
06	<u>Annual Financial Statement</u>	48
07	<u>Directors and officers</u>	58
08	<u>Glossary</u>	60
	<u>Colophon</u>	65



Foreword



“It’s important that the Netherlands innovates, takes its opportunities and quickly boosts national cyber-resilience.”

Roelof Meijer
CEO, SIDN



3

Why a strong internet matters

The internet is now integral to the way we live and work. We are using it more and more extensively and intensively. The coronavirus pandemic has driven a wave of ‘hyper-digitisation’, with many organisations accelerating their migration to online operations – some because they had no choice – and people using the internet more often and for more purposes. Because we have a good internet infrastructure, via which all manner of services are available, we can now do most things online: work, study, shop, watch performance art, visit museums, consult a doctor, do business, share a drink, do the cooking, celebrate birthdays and interact with family, friends and acquaintances. Some new online services may disappear again when the pandemic is over, but most are hopefully here to stay. As was the case the year before, the impact of the pandemic would have been far worse in 2021 without the modern internet.

One direct consequence is that we are becoming much more dependent on the internet. As a result, a trustworthy digital environment based on an open, accessible and secure internet is today more important than ever.

SIDN operates at the heart of the Dutch internet. The .nl domain is one of the world’s most secure internet domains and recognised by users as one of the most trustworthy. We are a private-sector organisation with a vital public role, responsible for the availability and quality of the .nl domain. Our journey towards problem-free, opportunity-rich digital living for everyone started thirty-five years ago, in 1986, when Dutch internet pioneer Piet Beertema sought permission to create the .nl top-level domain for the Netherlands. Ten years later, by which time there were 10,000 registered .nl domain names, he got together with Ted Lindgreen and Boudewijn Nederkoorn to set up SIDN. In the quarter-century since, we have developed into a successful and professional registry, now managing 6.2 million .nl domain names. We make all those domain names reachable via a DNS infrastructure, which forms the bedrock of our services and has been in non-stop operation for more than thirty-five years.

A wide range of stakeholders deserve credit for the success of .nl. They include all the registrants making active use of their .nl domain names, the



registrars helping people and organisations to register domain names, hosting their websites and enabling their e-mail traffic, and all the SIDN personnel working to make the .nl domain as secure and stable as possible. Every minute of every day, our drive and passion are directed towards promoting problem-free, opportunity-rich digital living for everyone in many different ways.

A real success, which would have been a disaster without the internet.

Growth of .nl

Het .nl-domein groeide de afgelopen 2 jaar flink. The .nl domain has grown considerably over the last two years. Since March 2020, the coronavirus pandemic has driven up demand for .nl domain names, resulting in a net growth rate three times that seen in 2019. In 2021, the number of new domain name registrations was again higher than forecast. In the first half year alone, the number of domain names in the .nl zone increased by 100,000. Furthermore, the anticipated upturn in cancellations one year on from the registration surge of spring 2020 did not materialise. In fact, the number of cancellations was slightly down. Our cautious conclusion is therefore that the accelerated migration to the internet is not a transient phenomenon.

As more and more businesses offer products and services via websites as well as using more traditional models, .nl's value to society continues to increase. We have seen start-ups and established enterprises opening new online channels, and wholesalers launching direct sales websites. A top-quality .nl domain offering high-grade services is consequently more important than ever.

Focus on cyber-resilience

Interest in digital security is growing – a development that we welcome, because safety has a major bearing on confidence in online services, social wellbeing and economic prosperity. Awareness of the importance of security extends beyond our industry. Digitisation featured prominently in the coalition agreement underpinning the new Dutch government, and the Netherlands now has its first State Secretary for Digitisation. The new administration is committed to utilising the “marvellous opportunities afforded by the digital revolution”, to fighting cybercrime, and to protecting fundamental civil

rights online. The coalition agreement signals the urgent need both for innovation and the use of opportunities, and for action to ensure the safety of people and organisations online.

That's very significant, because greater dependence on the internet brings increased vulnerability and more cybercrime. For example, the central conclusion of the [Cyber Security Assessment Netherlands 2021](#) was that “Cyber-attacks degrade the nervous system of our society.” Cyberthreats are changing and increasing year on year, but the resilience of companies, organisations and people in the Netherlands is not keeping pace.

Although regulatory intervention and supervision by the government are increasing, responsibility for cybersecurity remains largely with the organisations that might be targeted. Companies and other organisations, and people with their own businesses need to ensure that their security is on a sound footing. They must then build on that foundation to significantly raise their levels of cybersecurity and digital resilience.

We at SIDN are also working hard to boost the Netherlands' cyber-resilience. For example, we operate the SIDN BrandGuard monitoring service for companies, government agencies and other organisations, which will soon be extended to include logo detection functionality. We are active in the fight against fake webshops, and we help registrants to prevent data breaches with our new LEMMINGS system. We additionally support various outside organisations working in the field of internet security.

The internet of the future

Centralisation of the internet and its infrastructure and services is creating new challenges. Digital systems, such as DNS services and cloud storage, are increasingly developed and operated by a small number of big players based in the United States and China. A handful of online platforms such as Facebook and YouTube dominate our social landscape. The control that such players have over our knowledge, data and technologies now has significant drawbacks. The autonomy of Dutch and European internet users is consequently threatened, as are Dutch and European values and norms.

The problem of declining strategic digital autonomy is most tangible in the context of the nation's vital infrastructure, where outages can cause major social disruption. However, debate about the issue often overlooks our internet infrastructure, even though that infrastructure is essential to everything that happens online.



We are therefore looking at new internet properties and technologies that are better aligned with society's current and future reliability expectations. Our research team, SIDN Labs, has been active in the field since 2019, working with various partners on projects such as the Responsible Internet concept. The Responsible Internet is a security-by-design extension to the internet infrastructure that offers service providers and users greater insight into and control over their data traffic. The importance of the work was underlined this year, when the Dutch Research Council (NWO) made a sizeable grant to the universities participating in the project.

Impactful, forward-looking initiatives

Als beheerder van het .nl-domein vervullen we een voor de Netherlands, but also for the wider world. We contribute to infrastructural reliability and stability, and use various routes to invest in an innovative, accessible and futureproof internet. For example, we support promising initiatives through SIDN Fund, we undertake applied technical research at SIDN Labs, we participate in national and international forums, and we develop services in the fields of online identities and cybersecurity.

In relation to online identities, we made considerable progress with the development and implementation of IRMA, the open-source, decentralised eID platform that puts users in control of their personal data. In 2021, we lobbied for the eID system to be subject to tighter requirements under the proposed new Digital Government Act. That led to the announcement of an amendment that will reinforce principles such as open-source design and privacy by design. We assume that the Digital Government Act will pass into law and take effect some time in 2022. In the year ahead, we will therefore be working hard on IRMA's further development and pushing for statutory accreditation. We will also be looking to recruit partners to support the scaling up and adoption of IRMA. We are driven by the firm conviction that privacy by design and decentralised, open-source identity management based on solutions such as IRMA can make an important contribution to safe, convenient and opportunity-rich digital living.

2021: a jubilee year

Nederland bevindt zich in de digitale kopgroep. Where the internet is concerned, the Netherlands is a world leader. Our position at the forefront of innovation was reflected by a series of milestones reached in 2021. We had good reason to look back on

a history of achievement as the .nl domain reached the age of thirty-five, SIDN marked its twenty-fifth anniversary and SIDN Labs its tenth. We realised our operational goals for .nl and were again able to invest in the internet community through SIDN Fund, SIDN Labs and IRMA. As well as being a jubilee year, 2021 was an excellent operating year for SIDN.

Promoting confidence online through the Responsible Internet and eIDs designed for privacy.

Problem-free, opportunity-rich digital living

Yet 2021 was also a year when the pandemic continued to impact our lives. After a bleak start to the year, we twice hopefully reopened our offices, only for subsequent waves of infection to bring renewed restrictions and the disappointment of reclosure. The situation continued to ask a lot of everyone in the Netherlands and beyond, including our organisation, its personnel and their families, the registrars and our many partners. Nevertheless, we are able to look back on a year characterised by success. Although we faced challenges, they were nothing compared with the difficulties that some other sectors, individuals and organisations have had to contend with in the last two years.

While we are well equipped for staff to work from home, we look forward to having the team together again in 2022. We look forward to not merely working together, but also being together, to celebrating the landmarks passed last year, to once more being able to hold SIDN Inspire and to meeting our registrars and other stakeholders face-to-face again.

We firmly believe that a free, open, accessible and secure internet contributes to a better world for everyone. That conviction is the inspiration for everything we do.

We intend to maintain our development in 2022. The key aspects of an eventful year and our plans for the year ahead are described in this Annual Report. I hope you enjoy it.



Shortly before we completed the compilation of this annual report, just when it seemed that the pandemic's grip on our lives was loosening, Russian Federation army units launched a violent invasion of Ukraine. Within days, amid fears of the conflict spreading to EU and NATO members states, much of the world was preoccupied by this new crisis. Global condemnation of Russia and sanctions of many kinds soon followed. At the time of writing, however, there has been no consequent de-escalation. The conflict has already claimed thousands of civilian and military victims, and millions of Ukrainians have fled their homes, leaving everything behind. We have witnessed an exodus on an unprecedented scale.

Within our industry too, the response has been disbelief and horror. Ukrainian internet organisations have received offers of help from all sides. We and many of our European colleagues have offered our support to the registry for Ukraine's .ua top-level domain, for example.

However, the Ukrainian government's formal requests to ICANN and RIPE-NCC, that the former should remove the .ru domain from the root and that the latter should withdraw IPv4 and IPv6 addresses issued to Russian members, have been refused. The main arguments for refusal were:

1. The absence of a mandate for any private party to unilaterally decide to undertake the proposed course of action
2. Opposition to the principle of the internet infrastructure being used as a medium of sanction
3. The expectation that the requested sanctions would have little effect on Russian policy, but a much broader negative effect on the working of the internet
4. Fear that the proposed measures could lead to fragmentation of the internet

Ukraine's requests and the responses to them have led people to ask what the sector can do, and who has decision-making responsibility in that context. Discussion of those questions is by no means concluded, and my expectation is that there will be implications for the governance of essential internet infrastructure actors.

We will, of course, follow the EU's official sanctions policy. Otherwise, however, there is little that we can do other than offer help wherever possible and hope that the combination of diplomacy and sanctions brings about a swift end to the conflict.

Roelof Meijer,
CEO, SIDN



O I

A stable and socially valuable domain

A .nl domain that delivers value and embodies values

In May 2021, the number of .nl domain names moved past the 6.2 million mark. There was no cancellation wave, and the year was consequently an excellent year for SIDN in business terms. It appears that the migration to online trading was more than a transient phenomenon. At the start of the year, we signed a new cooperation agreement with the Registrars' Association (RA). We invested actively in co-funded marketing campaigns and developed a marketing toolkit for our registrars. We also proudly unveiled a new version of our SIDN Academy.



or

A stable and socially valuable domain

A .nl domain that delivers value and embodies values

Development of the .nl domain

Although growth of the .nl domain was not as strong in 2021 as the year before, the number of new .nl registrations was higher than expected. On 31 December 2021, there were 6,232,829 registered .nl domain names, 120,729 up on twelve months earlier. The growth was driven by both start-ups and established offline enterprises entering the online marketplace. Of course, many private individuals also register domain names for a wide variety of purposes. Over the year, a total of 896,236 domain names were registered, while 775,507 were cancelled. Most of 2020's new .nl registrants retained their domain names in 2021. Net growth was therefore 120,729, or 1.98 per cent.

High availability

In 2021, the availability of our DNS systems, which form part of the global Domain Name System (DNS) and the core of our services, was once again 100 per cent. Barely any of the maintenance undertaken on our registration system (DRS) involved perceptible

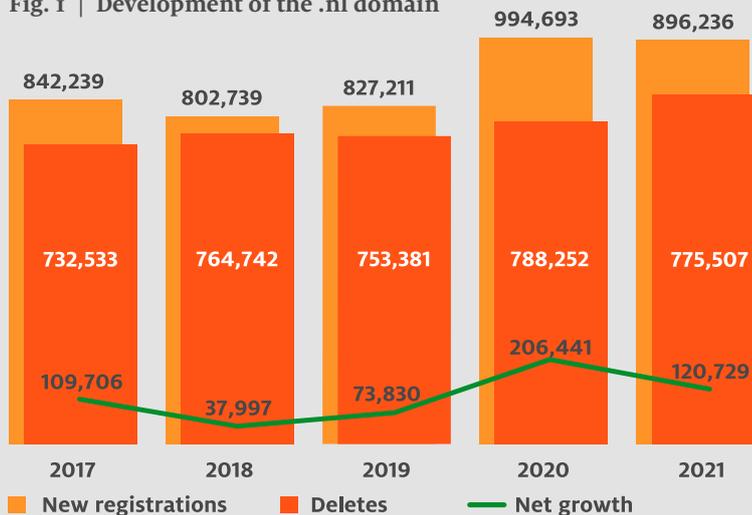
service interruptions, and all the work that did require downtime was completed within the predefined windows. However, despite taking a very careful approach to the replacement, patching and upgrading of equipment and systems, we did experience some unplanned outages. In light of those problems and other vulnerabilities, such as the vulnerability in the Apache Log4j software, we continue to work on improving our software, infrastructure, processes, procedures, testing facilities and integration and deployment methods.

Growth of .nl was again stronger than expected.

Market share

In the Netherlands, the domain name market is largely divided between .nl and .com. The .com

Fig. 1 | Development of the .nl domain





domain experienced strong growth in 2021, but not in the Netherlands or elsewhere in Europe. The .com domain's subdued performance here was attributable to it being particularly popular in the travel sector, which has been struggling with the effects of the coronavirus crisis for the last two years. By contrast, regional and local businesses have been performing well. Since such enterprises generally opt for .nl, the overall brand preference for .nl increased in 2021. Our market share for the year was 62 per cent. Usage of registered .nl domain names has also gradually increased. We believe that part of the explanation is that some businesses whose physical trading was affected by lockdowns used the opportunity to get websites up and running. Whereas in the past there was often an interval of six months between a domain name registration and the launch of an associated website, the interval in 2021 was typically just a few weeks.

Market developments

As indicated earlier, the factors driving continued growth of the .nl domain include low rates of cancellation and a migration to online commerce. In addition, many wholesalers have recently opened internet-based direct sales channels. There was growing realisation that offering products or services on a dedicated website could augment an established business model. That was illustrated as long ago as summer 2020, when we conducted a survey of new business proprietors. Every single respondent said they were planning an online presence. Another key development we have observed is that the importance of a unique, short and descriptive domain name has increased in the last ten years. According to domain name marketplace Sedo, since the start of the coronavirus pandemic many

businesses have demonstrated the value of a strong and sound domain name within the fast-growing e-commerce sector.

Cakes and celebrations

On 25 April 2021, shortly before King's Day – the Dutch national holiday celebrating the monarchy – the .nl domain reached the age of thirty-five. To mark the occasion, we ran a playful publicity campaign. People were invited to share their unique .nl domain names on Twitter, Facebook or Instagram, using the hashtag #ilovenl. Each of thirty-five lucky winners was sent a box of King's Day celebratory cakes. The campaign gave registrants the chance to showcase their businesses, while also raising the public profile of the .nl domain. For the rest of 2021, we continued to highlight recently registered .nl domain names with a series of blogs and vlogs telling the stories of the websites and businesses behind the names.

A strong and sound domain name is very important.

Price adjustment

Our prices remained unchanged from 2008 to 2021. However, we now find ourselves in a situation where no substantial percentage-terms growth is expected in the .nl domain, while registrar numbers are falling as a result of consolidation. The latter development implies registrars having larger domain name portfolios, leading to higher volume discounts

Fig. 2 | Market share in 2021

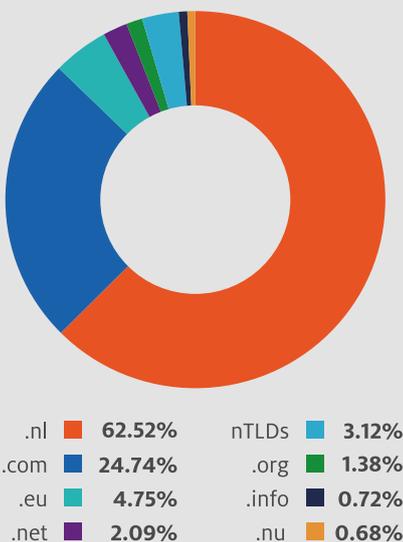


Fig. 3 | .nl price change over time (euros)

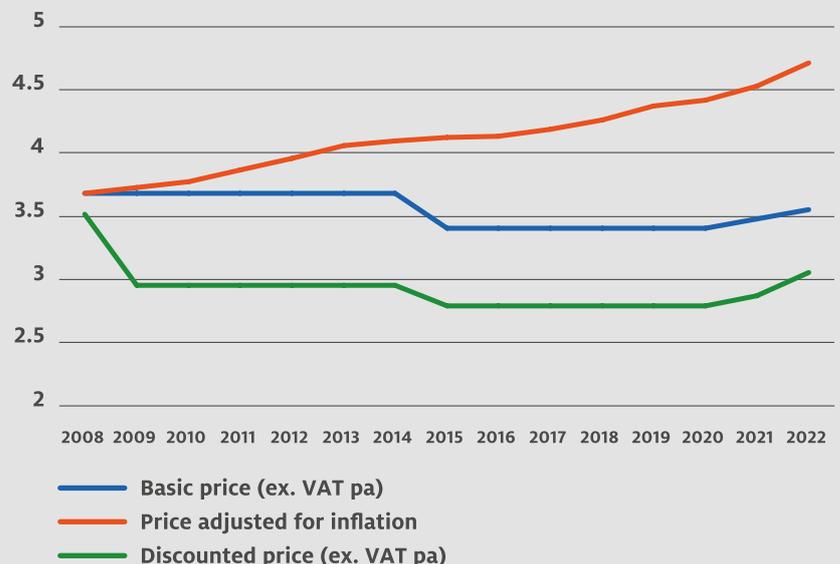
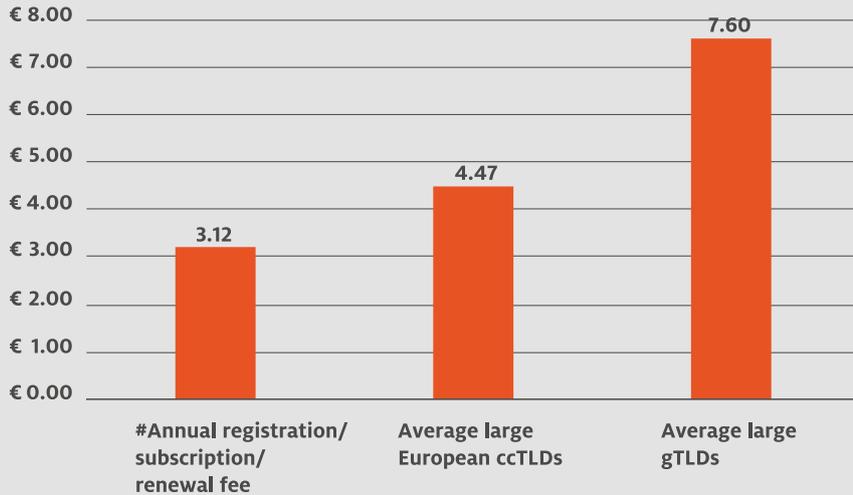




Fig. 4 | Price levels of .nl and peers (incl. discounts and registrar fees)



and bigger Registrar Scorecard reward payments. At the same time, our overheads are increasing, due to higher security costs and other factors. For example, expenditure on ICT has been rising by 3 to 4 per cent a year, partly because of investment in digital security and higher hardware prices driven by the global chip shortage. Against that background, we took the decision to raise prices by 2 per cent per year, starting in 2021. As a result, the price of a domain registration rose in 2021, from €3.40 to €3.48 per year. Nevertheless, a .nl domain name remains significantly cheaper than a domain name with one of the leading global extensions (.com or .org) or a country-code extension in most other European countries.

Developments in the registrar community

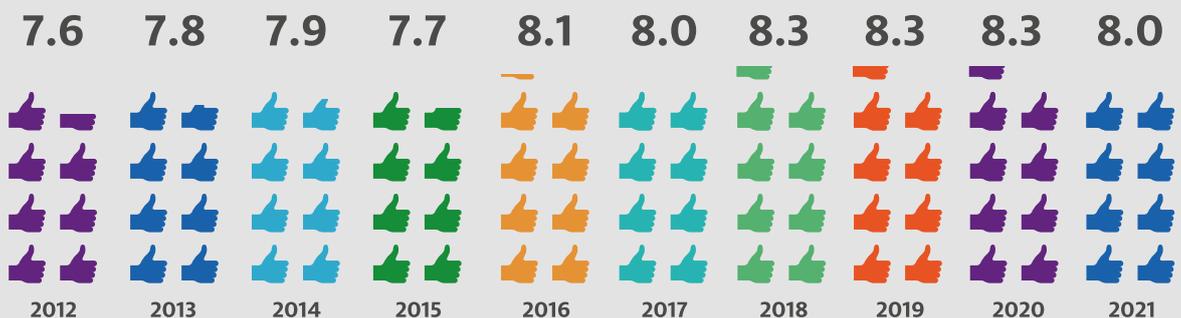
The Dutch registrar community is one of the biggest and most diverse in the world. However, a consolidation trend has been evident for a number of years. That continued in 2021, with the number of registrars falling from 1,054 to 993. Acquisitions and mergers enabled several of our registrars to make progress towards becoming major international players.

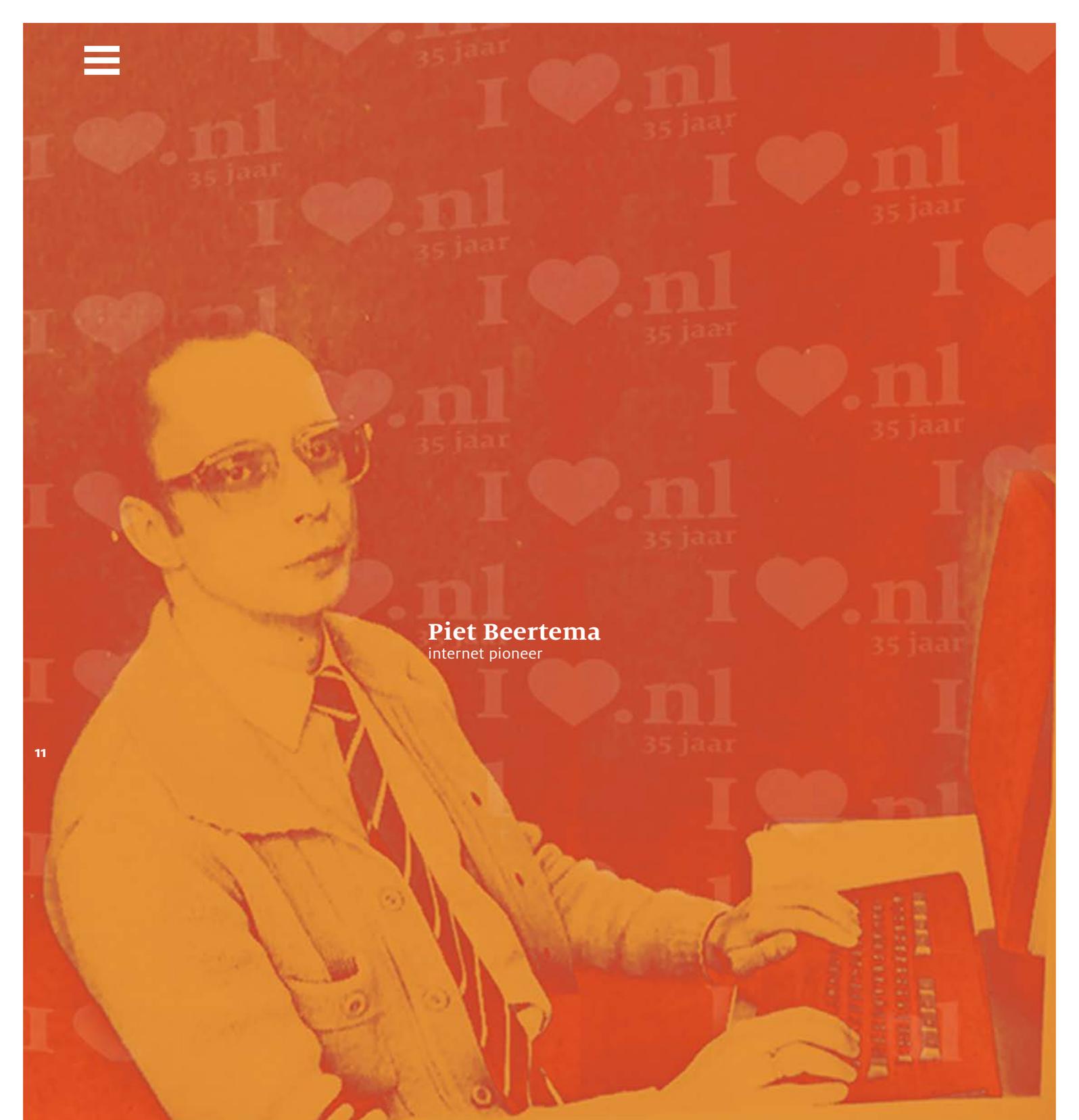
Registrar satisfaction remains high

In a survey held in 2021, registrars gave our services a mark of 8 out of 10. While that's a very creditable mark, it's down on the 8.3 we secured for the previous three years. The dip reflects disappointment occasioned by the price rise, access problems affecting our registrars' website, issues associated with the adoption of a new invoicing system, and the removal of some categories of information from the Whois. On the other hand, registrars remained very pleased with the personal contact experience provided by all parts of our organisation. Our various 'registrar projects' and our marketing support initiatives were also well received.

Registrars value our projects and marketing support.

Fig. 5 | Development in customer satisfaction





Piet Beertema
internet pioneer

11

35 years of .nl

One of the trailblazers who played a special role in creation of the .nl domain and SIDN is Piet Beertema. When working as Systems Administrator at the National Research Institute for Mathematics and Computer Science (CWI), he had the great idea of asking to establish the .nl top-level domain. Setting up a new TLD needed the approval of Jon Postel, a US internet pioneer. Piet received an e-mail giving him the go-ahead, and the .nl country code came into being on 25 April 1986. On 1 May 1986, the CWI registered the very first .nl domain name: cwi.nl. With that registration, .nl became the first active country-code domain outside the US. In 2021, we celebrated the thirty-fifth anniversary of our national internet domain. > [Read more on sidn.nl](#).

Co-funded marketing campaigns

Since late 2018, we have been offering registrars financial support with their marketing activities, subject to certain conditions. The aims of the policy are to encourage new .nl registrations and to promote .nl as one of the world's most secure and stable internet domains. All ten of the biggest .nl registrars made use of the scheme again last year. In order to make it more attractive to smaller registrars as well, we standardised the application process in 2021. An application form was made available on the SIDN website, so that registrars can easily request assistance with a proposed campaign. Another marketing support initiative was the launch of a .nl marketing toolkit for use by registrars and resellers, featuring rights-free images and copy. Over the year, our co-funded marketing activities yielded a total of 50,000 extra .nl registrations. When considering campaign proposals, we worked on the basis that the cost should be limited to three euros per extra domain name sold, in order to ensure that the scheme remained viable for both us and our registrars.

Co-funded marketing campaigns yielded roughly 50,000 new .nl registrations.

.nl Suggestion Tool and API key for registrars

A prominent feature of our website is the .nl Suggestion Tool. The tool enables visitors to easily check the availability of their ideal .nl domain names. If the checked domain is taken, the tool suggests alternatives that are still available, and invites the user to check out other ideas. Drawing on feedback from the RA and our customer consultation panel, we made further refinements to the Suggestion Tool in 2021. We optimised the search algorithms, increased the speed, and boosted the relevance of suggestions for the Dutch business market. With the aim of making the tool more user-friendly and intuitive, we also modified the design. The tool is now

accessible directly from the site's main menu and professional users have immediate access to Whois search functionality. For registrars, we developed an open-source API key. Extensive documentation and code templates were made available, making it easy for registrars to embed the suggestion tool in their own websites. About ten registrars are currently using the API.

Business intelligence platform

At the end of 2021, we unveiled SIDN Insights: a business intelligence platform currently available to a small pilot group of registrars. The platform gives users access to real-time information about the performance of their domain name portfolios. For example, there is data on domain name cancellations and how their portfolio quality – usage, security, cancellation rate, etc – compares with market norms. The aim is to help registrars make well informed business decisions about .nl and related products.

Cooperation with the RA

A new cooperation agreement with the RA took effect on 1 January 2021, which was extended for a further twelve months at the end of the year. On many .nl-related issues, cooperation was very constructive. The RA provides us with advice, represents the interests of their thousand or so members, and promotes effective collaboration between ourselves and the .nl registrars. We compensate the RA financially for its time and input. Last year, we worked closely with the RA in fields such as marketing and communication activities. The RA launched an online portal for the exchange of documents and messages. The new cooperation agreement is based on respect for each party's independence. In October, we amended Article 16 of our General Terms and Conditions for Registrars, which relates to RA membership. New registrars are no longer automatically enrolled as RA members, and registrars are now responsible for paying their own membership fees. We covered the cost of registrars' automatic membership until October 2021.

Funding of projects that benefit registrars

Since 2018, we have funded projects that help to enhance the .nl domain and have commercial benefits for .nl registrars. The projects in question are developed in collaboration with the RA. In 2021, we unveiled a new version of our SIDN Academy and continued our existing projects.

Some examples of registrar projects

Hosting Infracan

Many .nl registrars or their resellers provide hosting services. The security of the technical infrastructures used to deliver such services has a significant bearing on the security and reliability of the .nl domain and the wider internet. We therefore partnered with ThreadStone and the RA to develop

the Hosting Infrascan, launched in 2020. The service enables .nl registrars and hosting firms to get their technical infrastructures scanned for vulnerabilities at a modest cost, so that corrective action can be taken where appropriate. We cover the bulk of the cost of the Hosting Infrascan. In 2021, about thirty-five registrars made use of the service and more than 350 servers were scanned.

Legal Help Desk

Sinds 2018 bieden we een juridisch loket aan voor registrars die bij de VvR zijn aangesloten. Since 2018, we've been running a Legal Help Desk service for RA-affiliated registrars. The service offers registrars swift, free answers to questions about privacy, terms and conditions and other issues involving ICT and the law. The Help Desk is an independent service facilitated by the legal consultancy ICTRecht.

VPN whitelisting for the DRS

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

SIDN Academy

After two successful offline editions of the SIDN Academy, we launched an online version in 2020. The Academy provides .nl registrars with training on topics such as the DNS and modern internet standards. Making training available online enables us to increase the reach and impact of the Academy. In 2021, we upgraded the existing modules and added a new module on internet abuse. We also started the development of a module on IPv6, which we plan to make available in early 2022. Nevertheless, for understandable reasons, we were unable to realise our goals for 2021. The SIDN Academy is an initiative organised in collaboration with the RA. Use of the Academy is free for .nl registrars. In due course, we intend to make the programmes available to a wider audience on a low-threshold paid basis. Any income generated will be re-invested in the further development of learning modules.

Registrar Scorecard

The Registrar Scorecard (RSC) is a scheme that offers registrars incentives for contributing to the quality of the .nl zone. The RSC has demonstrably improved the security of the .nl domain. The 191 registrars that participate in the RSC account for a combined total of 90 per cent of the .nl zone. In 2021, we used the RSC to promote the adoption of IPv6, DNSSEC, StartTLS, DANE, DMARC, DKIM and SPF. Growth in the number of domain names supporting the DANE e-mail standard flattened off considerably.

However, the number of IPv6-enabled .nls increased slightly, from 2.119 million to 2.127 million. Meanwhile, use of StartTLS went from 724,000 to 814,000 domain names, and support for DMARC from 1.357 million to 1.525 million. Through the RSC, we paid incentives totalling €1.128 million to participating registrars in 2021. During the year, we temporarily made the DNSSEC incentive additionally dependent on AAAA and HINFO record checks..

SIDN Panel

As operators of the .nl domain, we attach great importance to the views of internet users and registrants on topics such as internet use, security and privacy. In June 2021, therefore, we successfully introduced the SIDN Panel. The Panel was established with the aim of achieving the best possible alignment between our services and the wishes of .nl registrants and the Dutch internet community. The panel now has more than 250 members, who are regularly invited to participate in short surveys, enabling us to quickly test ideas and fine-tune initiatives. The average response rate is 40 per cent, and within forty-eight hours we are able to gather enough feedback to inform our decision-making.

Fig. 6 | Development in the number of DNSSEC-enabled domain names (x 1,000)

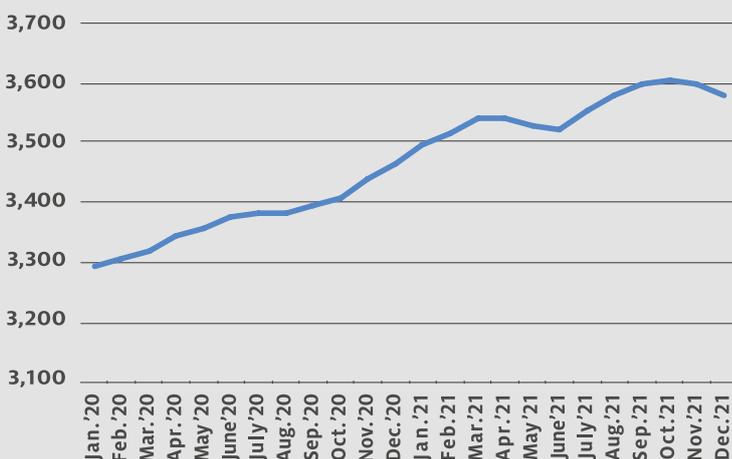


Fig. 7 | IPv6-enabled domain names (x 1,000)

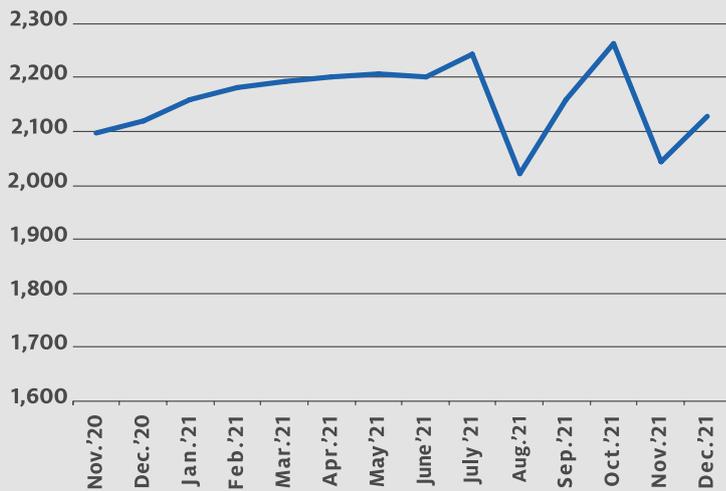
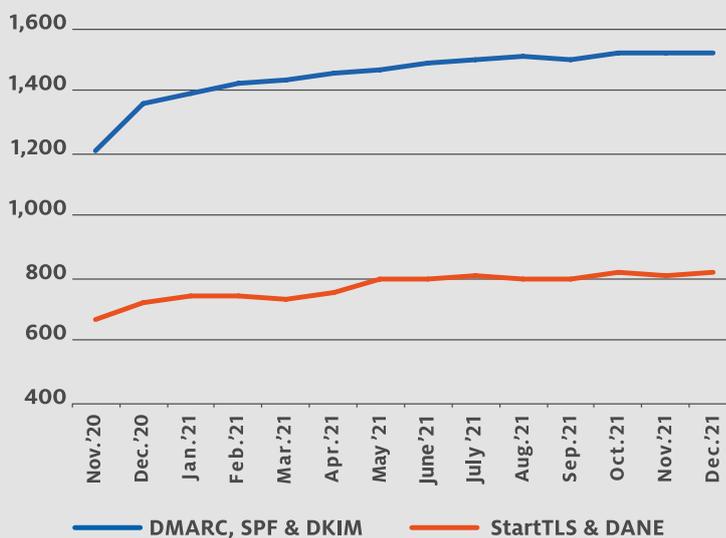


Fig. 8 | Use of e-mail security standards (x 1,000)



Complaints and Appeals Board

In most cases, the registration and assignment of .nl domain names goes without a hitch. From time to time, however, a registrar or a .nl registrant is unhappy with a decision that we make. In such cases, the registrar or registrant can appeal to the Complaints and Appeals Board (C&AB). The C&AB is an independent body that also considers complaints about domain name registrations that are believed to be inconsistent with public order or decency. In 2021, the C&AB received one appeal: a .nl registrant disagreed with SIDN's decision to assign a domain name to another party. The C&AB is expected to rule on the case in early 2022. The C&AB's rulings are published on cvkb.nl.

DomJur.nl

DomJur.nl is a website where, until October 2021, Tilburg University's Faculty of Law and SIDN jointly published Dutch court rulings and articles relating

to domain names in general and .nl domain names in particular. Decisions made in the context of the notice-and-take-down scheme are also reported on the website. In mid-October, the website was transferred to legal information publisher deLex Media. Under deLex's management, a modified version of the site will continue publishing jurisprudence as it becomes available. The DomJur.nl database remains publicly accessible.

Dispute Resolution System for .nl Domain Names

In 2021, sixty-eight cases were referred to the WIPO Arbitration and Mediation Center under the Dispute Resolution Regulations for .nl Domain Names. Thirty-two 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. Seven cases are still under consideration. Our mediators handled twenty-four cases. In twelve 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 sixty-one notice-and-take-down requests in 2021, relating to malpractices such as identity fraud and the sale of imitation products. Twenty-one 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.

Registry services

As well as being the registry for .nl, we provide registry services for three other top-level domains: .aw (Aruba), .amsterdam and .politie. The latter two are 'generic' top-level domains. For all three domains, the availability of our domain name resolving (DNS) services was 100 per cent in 2021.

New gTLD applications

Subsequent Procedures Policy Development Process working group ('SubPro') submitted its Final Report, setting out recommendations on a fresh application window for new gTLDs. In the second half of the year, ICANN initiated the Operational Design Phase, during which the practicalities of the application process will be decided. We continue to monitor developments carefully.

Supervision by the Radiocommunications Agency

In 2018, we were designated an operator of essential

services (OES) under the Network and Information Systems Security Act. As such, we became subject to supervision by the Radiocommunications Agency. The Agency carried out its first audit of our work in 2020, using our ISO27001 certification framework as its basis. The findings of the Agency's audits will help us further enhance the security of the .nl domain. In 2021, the Agency carried out a follow-up audit. With the exception of a few action points, no matters of concern were identified.

Investigation by the Ministry of Economic Affairs and Climate Policy

In response to expressions of concern in the media and representations made by the Registrars' Association, the Ministry of Economic Affairs and Climate Policy began an investigation in the summer of 2021, with our cooperation. The investigation is linked to and anticipates the extension of our covenant with the Ministry in 2022. The central question under consideration is, 'What activities is SIDN developing in addition to the issue and administration of .nl domain names, and do such activities entail any risk to the continuity and stability of the .nl domain?' Assurance of the continuous availability of .nl and the separation and mitigation of risk are our absolute priorities. As an independent, private organisation, SIDN is of course free to establish other activities that are not directly related to .nl. We recognise the importance of separating any associated risks, such as liability risks. Publication of the investigation findings is expected in 2022. We have every confidence that the central conclusion will be that we are doing all we can to mitigate risks to the continuity of .nl.

Outlook for 2022

European NIS2 Directive

Within the EU, the first Network and Information Security Directive (NIS1) is currently in force. The Directive is implemented in Dutch law by the Network and Information Systems Security Act, under which SIDN has been designated an operator of essential services (OES). In 2020, the European Commission published a proposal for a second directive, NIS2, to supersede NIS1. The precise content of NIS2 is not yet clear. However, the draft version of NIS2's Article 23 includes provisions creating certain legal duties that would have implications for the domain name industry. For example, European registries and registrars would be expected to do more to ensure the accuracy of the data they hold regarding registrants. In the years ahead, NIS2 could have a major impact on registrars and on registries, including SIDN. In anticipation of

the proposed directive, we are working with the RA, our registrars and other registries to explore ways of efficiently and effectively complying with the new requirements. We see the rollout of electronic identities (eIDs) and authentication platforms such as IRMA as being very valuable in that context. Such technologies can support the identification of registrants and the automatic verification of data.

New incentives added to the Registrar Scorecard

Since its introduction in 2015, the RSC has had a positive effect on the use of secure internet standards and IPv6. Indeed, the impact on DNSSEC adoption has been huge. Although the growth of support for the standards covered by the RSC was slight in 2021, we plan to maintain the current incentives in 2022. However, we are cutting the IPv6 incentive payable per domain name by €0,02. We will revert to determining eligibility for the DNSSEC incentive by performing HOST information and NXDOMAIN checks. The incentive programme will be evaluated in 2022, when we will consider whether our chosen means of promoting adoption remains the most appropriate. We are additionally working on short-term incentives designed to yield quick wins in certain fields. Our aim is to launch the first such incentive in the middle of 2022.

Support for registrars

An important focus in 2022 will be supporting registrars' marketing activities. We will also continue to seek input from customers for use in market analysis, and address the points identified by the Registrar Satisfaction Survey as warranting attention. In addition, we plan to invest in raising the profile of projects that can help to improve .nl, particularly amongst smaller registrars. Other goals for 2022 include working with the RA to improve the business and financial data made available to registrars, and upgrading our applications' user management and sign-on arrangements.

.nl Suggestion Tool

Our primary focus in 2022 will be increasing the number of .nl Suggestion Tool users. More users will mean more data on the tool's performance, thus facilitating the process of refinement. We will also be working to improve the quality of the suggestions made by the algorithm, so that it's even easier for users to quickly find their ideal .nl domain names.

Reduction of direct debit discount

As in 2021, our .nl registry fees will be rising by 2 per cent in 2022. Anyone who registers a .nl domain name in 2022 will therefore pay €3.55 for their first twelve months. The registrar's account fee



will rise to €71 per month. At the same time, we are reducing the direct debit discount from 5 per cent to 2.5 per cent. The changes are necessitated by year-on-year rises in our overheads, such as security costs and digital infrastructure maintenance costs.

Covenant with the Ministry of Economic Affairs

We have a covenant with the Ministry of Economic Affairs, which was originally agreed in 2008 and renewed in 2016 for a further seven years.

The covenant formalises the arrangements by which we and the Ministry together ensure the availability of the .nl domain. In it, we also commit to maintaining the .nl domain's association with the Netherlands. The existing covenant expires in 2022, and we are therefore in talks with the Ministry about its renewal.



Joost Pisters

Product Strategist, Argeweb/Yourhosting



Koen van Deudekom

CEO, Argeweb/Yourhosting

Preventing security incidents

Sensitive data can be compromised if a cancelled domain name continues to attract mail traffic and the name is later re-registered by someone else. In recent years, various organisations have been caught out that way, with private information getting into the wrong hands. We therefore wanted to find a way of helping organisations and individuals avoid cancellation-related security breaches. That led to SIDN Labs prototyping a system called LEMMINGS (deLetEd doMain Mail warNinG System). In partnership with Joost and Koen at .nl registrar Argeweb, we set up a pilot to evaluate LEMMINGS. Koen van Deudekom: "Customers tend to be unaware of the full implications of domain name cancellation, in terms of lost value and risk exposure. LEMMINGS addresses that problem by promoting awareness. We would like to see it rolled out for the whole .nl zone."

> [Read more on sidnlabs.nl](https://www.sidnlabs.nl).



02

Impact in two domains

Successful services in the fields of online identity and cybersecurity

With a view to contributing to problem-free, opportunity-rich digital living for everyone, we actively seek answers to societal problems in fields such as cybersecurity and online identity. For example, we work with partners on the introduction of new products and services with the potential to make the internet safer and more convenient. We are looking to extend the rollout of the privacy-friendly IRMA identity platform and make decentralised identity management a success. In 2021, we transferred CyberSterk, the security service for SMEs, to an outside entity, and we continued to expand our Domain Name Surveillance Service under the new name of SIDN BrandGuard.



02

Impact in two domains

Successful services in the fields of online identity and cybersecurity

Online identity

Digital Government Act

In 2021, we lobbied for the eID system to be subject to tighter requirements under the proposed new Digital Government Act. In response, an amendment has been put forward, which will provide a stronger legal basis for the fundamental criteria that we believe an eID system should meet – privacy by design, open-source design and decentralisation. Meanwhile, at the European level, there are moves to create a digital identity system for all European citizens, based on eIDAS. The framework proposed by the European Commission is very much in line with our own values and the philosophy on which the IRMA app is based.

IRMA and IRMAconnect

Secure and convenient digital identities are very important for private citizens and organisations alike. The privacy-friendly, open-source identity platform IRMA – an acronym derived from I Reveal My Attributes – is the only current eID system that is entirely in keeping with our vision. The free IRMA app enables users to gather authenticated identity data and store it on their smartphones. When interacting with service providers – logging in to a website or signing a digital document, for example – they can then limit the information that they share, revealing only the items ('attributes') that are strictly necessary.

IRMA is a decentralised system, meaning that personal data isn't stored centrally, but only on the user's phone. That enables the user to retain

their privacy and frustrate service providers' efforts to profile them. IRMA was created by Bart Jacobs, Professor of Computer Security, Privacy and Data Management at Radboud University. The platform was later transferred to the Privacy by Design Foundation. We entered into a strategic partnership with Privacy by Design in 2018, under the banner of 'IRMA powered by SIDN'. Since then, we have been working to reinforce IRMA and support the platform's further development. We operate the IRMA backbone, assure the platform's financial continuity and realise IRMA-based innovations. We also provide a service called IRMAconnect, which helps organisations get started with IRMA.

The IRMA app passed the milestone of 50,000 users.

In 2021, the IRMA app passed the milestone of 50,000 users. The progress reflects the growing interest in secure online identification where the user retains control of their personal data. Over the last year, we have sought to refine and grow IRMA in various ways. Several developers from the Privacy by Design Foundation joined our payroll, and IRMA's technical infrastructure is now operated by our data centres. We also took steps to recruit end users, organisations willing to issue authenticated personal data and organisations interested in adding IRMA



Michiel Geerdink

CEO, Zynyo



20

Signing digital documents with IRMA

In 2021, Zynyo enabled IRMA authentication on its digital signing platform. “We are constantly looking to add new, privacy-friendly authentication options to our platform with the aim of boosting access to and trust in digital signing. IRMA is an exceptional authentication medium that further enhances our platform. It can interact with various sources to fetch authenticated data specific to the signatory,” said Michiel Geerdink.

The integration of IRMA into the Zynyo platform underscores the great potential of IRMA. We firmly believe that IRMA is the most ethical and trustworthy public and private identity solution available; a solution that truly puts user privacy first. > [Read more on sidn.nl](#).



support to their systems. With the aim of making the IRMA app more user-friendly and meeting the requirements of the anticipated Digital Government Act, a redesign process was set in motion, which will continue in 2022. In 2021, the digital signing platform Zynyo integrated IRMA into its services. We now use Zynyo's IRMA-enabled service for internal document signing. Adoption by Zynyo illustrates IRMA's potential and the importance of secure authentication.

Cybersecurity

SIDN BrandGuard

In November 2021, we renamed our Domain Name Surveillance Service, which became SIDN BrandGuard. The new name is a better reflection of what the service entails: the protection of internet users. SIDN BrandGuard is a monitoring service that now helps the companies and organisations behind three hundred-plus leading brands to protect themselves and their customers against reputational damage and phishing. Subscribers are informed about domain name registrations that include their brand names, both in the .nl domain and in other domains all around the world, including .com. The service also enables users to oversee registrations made by their own company or group and by business partners, and thus prevent reputational damage and high costs.

can be initiated with a view to getting control of an offending domain name or preventing its use. In the middle of the year, we also launched DBS Feed 2.0, now renamed SIDN Datafeed, which is synchronised with the SIDN BrandGuard web interface. The user interface was upgraded as well to make it clearer and more convenient. We additionally welcomed a number of new subscribers to the enhanced service.

With SIDN BrandGuard, we protect more than three hundred brand names.

CyberSterk

We are constantly investigating potential threats to internet security. In 2018, we identified low levels of cyber-resilience amongst SMEs as an area of concern. That led to the following year's introduction of CyberSterk: a low-threshold service that gives SMEs a clear picture of their e-security status. CyberSterk scans websites and networks for vulnerabilities, presents detected issues on a user-friendly dashboard and suggests solutions. We launched the service with the aim of helping SMEs protect themselves against cybercrime. It was ultimately decided that the best way to realise the great potential of the service was to transfer CyberSterk to Guardian360 and SecureMe2, two partners who had been involved with the initiative from the outset. On 1 April 2021, they took over responsibility for CyberSterk with the aim of accelerating its growth. The new operators are now receiving a steady flow of requests from SMEs looking to use the CyberSterk service.

Outlook

Digital Government Act

In 2022, we will continue working to influence the proposed Digital Government Act, with the aim of persuading the government to make admission to the eID system conditional upon respect for the principles of privacy by design, open-source design and decentralisation. We believe that those principles should be fundamental to an eID system. Consideration of proposed amendments is likely to delay enactment of the legislation until at least the middle of 2022.

In early 2021, we extended the SIDN BrandGuard service by adding a legal follow-up mechanism. The new feature lets a subscriber obtain legal advice and initiate action in response to the use of their brand name in a domain name. With the help of specialist lawyers, follow-up action and proceedings

Fig. 9 | Number of brands protected by SIDN BrandGuard





IRMA

We are working to ensure that IRMA is ready for accreditation under the Digital Government Act. Accreditation will allow the use of IRMA as a means of accessing both public and private services. In the meantime, we will continue refining IRMA. For example, we plan to roll out a redesigned IRMA app in 2022 and upgrade the IRMA website. We are also working to organise IRMA use cases and pilots with various companies and other organisations. To that end, we are in discussion with a range of libraries, educational institutes, government agencies, insurance companies and others. Another goal for 2022 is to identify partners willing to underwrite the rollout of IRMA.

SIDN BrandGuard

In 2022, we intend to add logo detection functionality to SIDN BrandGuard, utilising the LogoMotive technology developed by SIDN Labs. Subscribers will then be able to get information not only about domain names that may infringe their rights, but also about potentially unauthorised use of their logos. Logo detection will be available to existing and new BrandGuard users as an expansion module. We also want to offer users greater flexibility, for example by allowing them to enter their own domain names and thus build an overview of their domain name portfolios. SIDN BrandGuard's added value for SMEs will be highlighted as well. Given that many smaller businesses have no brand protection, we envision a key role for SIDN BrandGuard in this sector. We will accordingly be looking to develop a service tailored to the needs of SMEs.



03

Profit with a purpose

Investment in the Dutch and international internet communities

SIDN is a non-profit organisation. We endeavour to secure a responsible, positive return on the operation of .nl, SIDN BrandGuard, IRMA and certain other investments. That is necessary to enable us to continue to innovate and to maintain an adequate financial buffer, and especially to enable us to continue investing in problem-free, opportunity-rich digital living for all. Through SIDN Labs, we work to improve the reliability of the internet infrastructure by undertaking applied technical research and developing new technologies and know-how. We devise ways of tackling internet abuse, for example, as well as undertaking large-scale internet measurement campaigns and contributing to the development of new, secure internet systems for the future. Through SIDN Fund, we invest in projects with real value to the community that help to make the internet stronger and its users more resilient. We also share our knowledge, collaborate with universities, colleges and other players, and play an active role in various international forums.

03

Profit with a purpose

Investment in the Dutch and international internet communities

Tackling internet abuse

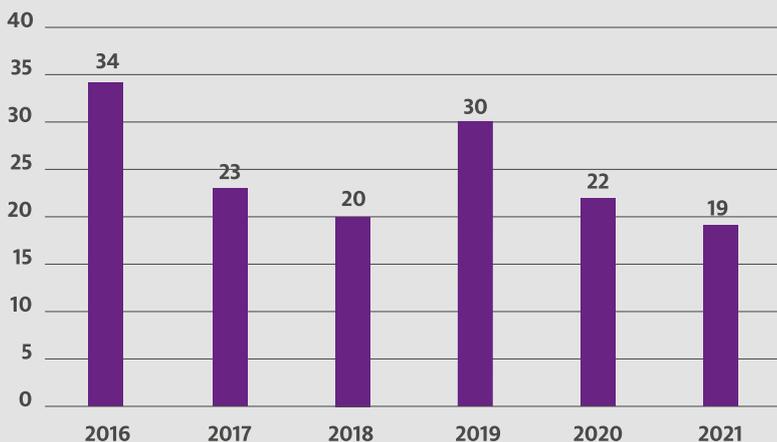
The .nl domain is one of the most secure top-level domains in the world (see, for example, [Study on Domain Name System \(DNS\) Abuse and Scamadvisor](#)). In order to protect that status, we work to tackle abuse of the internet in various ways.

Abuse204.nl ('abuse to zero for .nl') is a programme designed to prevent phishing and malware in the .nl zone. Run in partnership with registrars and hosting service providers, the programme is intended to make .nl domain names unattractive to cybercriminals. Abuse204.nl alerts registrars and hosting service providers to suspected abuse on their networks, enabling them to intervene. We succeeded in cutting the average lifespan of phishing sites and malware sites to less than twenty hours in 2021. We are also active in

the fight against fake webshops and other forms of abuse involving .nl domain names. Sometimes, in order to prevent abuse, we have to intervene by disabling a domain name. Legal proceedings started by others can also lead to us being asked to take action or share information. We believe it is important to be open and transparent about such interventions, because they can have major implications for those involved. Since 2020, we have therefore been publishing quarterly transparency reports on our website. > For details, see [sidn.nl](#).

.nl is one of the most secure top-level domains in the world.

Fig. 10 | Average up-time of phishing sites and websites with malware, in hours



Another important field of activity is the promotion of secure internet and e-mail standards. We pursue our goals in that field by, for example, offering financial incentives to registrars and sharing our knowledge through the SIDN Academy and other channels. On our website, we also provide hands-on guides to the implementation of e-mail security standards, such as DKIM, DMARC and DANE. In 2021, we published a maturity model explaining the interrelationships and interdependencies between modern internet standards, and suggesting priorities. > For details, see [sidn.nl](#).

Research partnership with TUCCR

Major cyber-attacks on universities, local authorities and companies are increasingly common. Unfortunately, not enough is yet known about cybersecurity to prevent such attacks, and there is insufficient sharing of the knowledge that does exist. With a view to bringing about change, the Twente University Centre for Cybersecurity (TUCCR) was established in March 2021.

TUCCR is a collaborative data and network security initiative through which science, government and the business community are brought into direct contact. It also works to make research findings suitable for use in new cyber security products, services and policy. TUCCR seeks to achieve societal impact by combining fundamental and applied research. It is the brainchild of two professors, Willem Jonker and Aiko Pras.

We were one of TUCCR's co-founders and we remain a partner, providing both financial and practical support.

Landing pages for disabled websites

Since January 2021, we have been intervening in cases where .nl domain names are reported to the Police National Internet Fraud Desk (LMIO). At the LMIO's request, we approach the registrant of each reported domain name, with a view to verifying the registration data. If verification is not obtained, we change the name servers so that the domain name points to a landing page with information explaining why the site is no longer reachable. The use of the landing pages helps to make internet users aware that not all webshops and sites are trustworthy. In 2021, there were about fifty such cases.

Participation in the national cyber-emergency drill

It is very important that we increase national resilience to the growing threat of cyber-attack. In June 2021, the National Cyber Security Centre (NCSC) and the National Coordinator for Security and Counterterrorism (NCTV) therefore organised the biggest cyber-emergency drill ever held in the Netherlands: ISIDOOR 2021. The exercise involved about ninety-six vital infrastructure operators.

Having been designated an operator of essential services (OES) in 2018, we took part in ISIDOOR for the first time in 2021. During the exercise, various cyber-incidents were simulated. Lessons learnt will be reflected in participating organisations' cyber-incident preparations and incorporated into plans and procedures such as the National Cyber-emergency Plan. As well as reassuring us that we are generally well-prepared, the exercise also flagged

up a small number of areas where we could do even better. Our systems and processes have since been upgraded accordingly.

SIDN took part in the biggest cyber-emergency exercise ever held in the Netherlands.

SIDN Labs

A secure, resilient and transparent internet infrastructure is of increasing social and economic importance. Our research team, SIDN Labs, therefore works to continue increasing the security, resilience and transparency of that infrastructure for the Netherlands, Europe and the wider world. It does so by performing large-scale internet measurements and analyses, developing prototypes and testbeds, and contributing to the development of secure, modern internet standards. SIDN Labs also publishes its research findings, e.g. in the form of articles, reports and software.

SIDN Labs collaborates with universities, infrastructure operators and other research centres. By doing so it aims to build bridges between the academic and operational worlds, and thus increase the reliability of the internet infrastructure. SIDN Labs' research partners include the University of Twente (UT), Delft University of Technology (TU Delft), the University of Amsterdam (UvA), NLnet Labs, SURF and the University of Southern California. In 2021, SIDN Labs staff also gave lectures at TU Delft, UT and UvA.

tsuNAME: serious DNS vulnerability localised and resolved

In early 2021, a joint measurement study by SIDN Labs, InternetNZ (the registry for New Zealand's .nz domain) and USC Information Science Institute in the US revealed a vulnerability in the DNS, which they called tsuNAME. The vulnerability meant that malicious actors could potentially use DNS resolvers to mount large-scale DDoS attacks on top-level domains and other authoritative DNS operators. After careful analysis, the researchers concluded that 3,600 resolvers distributed across about 2,600 networks were susceptible to the problem. They included globally popular public resolvers, such as Google Public DNS and Cisco Open DNS. The



researchers followed a responsible disclosure process, which involved asking DNS server and resolver operators to check their systems' status and, where necessary, rectify the situation urgently. Google and

Cisco fixed their resolvers, with the research team helping Google to address the vulnerability on Google Public DNS.

Some of the projects undertaken by SIDN Labs in 2021

Responsible Internet

The strategic digital autonomy of the Netherlands and Europe are under threat. We are increasingly dependent on digital systems – network equipment, DNS services and cloud storage – that are made, operated or owned elsewhere, such as the US or China. As a result, such players have more and more control over our knowledge, data and technologies, while we have less and less. Such problems are widely recognised in relation to artificial intelligence, cloud storage, critical infrastructure and other such fields, but not in relation to the internet infrastructure.

In response, SIDN Labs and a number of partner universities and internet operators developed the Responsible Internet concept in 2020. The thinking behind this security-by-design extension to the internet infrastructure is to give users more control over their dependencies on the internet. That would be achieved by, for example, increasing users' insight into the structure and properties of the internet and how their data is routed. With more information available to them, users could decide how they wish to communicate, and therefore protect themselves. We envisage the technological base of the Responsible Internet being formed by open programmable networks consisting of open hardware modules and devices running open-source software.

The importance of the work was underlined this year, when the Dutch Research Council (NWO) made a grant of 1.9 million euros to fund a small-scale Responsible Internet development project based in the Netherlands. The money will enable the participating universities to assign seven PhD students to the work.

At SIDN Labs, we developed and published our prototype SCION router written in P4, a programming language for network equipment. SCION (Scalability, Control and Isolation on Next-Generation Networks) is an internet technology that we see as a possible mechanism for realisation of the Responsible Internet. In line with that vision, we also developed a well-received interactive exercise for the University of Twente's Advanced Networking course. By completing the exercise, students are able to see for themselves how a SCION-based internet would increase user control over network paths.

A key principle of the Responsible Internet is that it should retain the existing technical internet values, such as openness, universal access, and decentralised and distributed network ownership and control.

We are working hard on a strong internet for the future.

DDoS Clearing House

It is very important that we make the Netherlands more resilient to large-scale DDoS attacks in order to protect ourselves against serious social disruption. The number of DDoS attacks rose again in 2021. However, a collective response to the problem remains lacking. Cooperation based on the sharing of attack-related data and expertise would increase organisations' ability to learn quickly and take a more proactive approach to defending themselves.

In 2021, we therefore worked with our partners in CONCORDIA and the Dutch Anti-DDoS Coalition to further improve the DDoS Clearing House. The Clearing House is a system through which participating organisations automatically share 'DDoS fingerprints' – distinctive attack profiles – with one another. SIDN Labs and SURF jointly developed a testbed for running realistic trials with the Clearing House.



Both the Clearing House itself and the testbed are being developed under the umbrella of the European CONCORDIA project. The Clearing House will ultimately be deployed within the Dutch Anti-DDoS Coalition.

At the start of 2021, the European Commission selected the DDoS Clearing House for inclusion in its Innovation Radar. The move recognised the Clearing House as an experimental innovation with great potential for increasing collective resilience to DDoS attacks.

It is very important that we make the Netherlands more resilient to large-scale DDoS attacks.

Anycast testbed

Since 2020, we've been running the Anycast2020 testbed at SIDN Labs. We use this SIDN-designed and managed anycast setup to investigate ways of maximising the flexibility and cost-efficiency of a global anycast infrastructure. Anycast2020 is intended to serve as a blueprint for a new operational anycast infrastructure for our .nl services.

In 2021, we linked up with the University of Twente to develop the Tangled open anycast testbed. The aim is to facilitate experimental anycast research by saving researchers the trouble of setting up their own test infrastructure. Because Tangled is specifically intended to help network researchers, we see it as a useful supplement to our own Anycast2020 testbed.

Anteater

DNS operators aim to get DNS responses to internet-enabled devices, such as smartphones and laptops, as quickly as possible. Response speeds are essential to the performance of browsers, mail programs and other apps. However, it is difficult for DNS operators to know what delays devices encounter in practice, because the operators have no knowledge of what networks their users' devices are using.

We have therefore developed a tool called Anteater, which allows DNS operators to monitor response times all across their authoritative DNS infrastructures. To do that, Anteater makes use of ENTRADA, our open-source DNS data streaming warehouse. During the year, we converted Anteater into an open-source tool, so that other DNS operators can use it to help improve the stability of the entire DNS.

IoT security

The Internet of Things (IoT) is growing rapidly. That introduces certain challenges, because many IoT devices aren't secure. Another problem is that users often can't see what information an IoT device is collecting, or who that information is shared with.

We therefore developed an open-source platform called **Security and Privacy for In-home Networks (SPIN)**. Its purpose is to help users and researchers to analyse the behaviour of IoT devices and other network equipment. SPIN inspects the network traffic associated with IoT devices connected to a network 'at the edge' of the internet, e.g. in a home network. It also enables software users to exercise more control over their IoT devices and the data that the devices are sharing.

In October 2021, we launched SPIN 1.0, a stable version of SPIN with various new features. One feature of the new version is 'bridge mode' functionality, making it easier for users to install SPIN on their networks. We also improved SPIN's web interface and the way SPIN imports network traffic using the PCAP reader. The software helps to make the IoT more transparent for users.

With the release of SPIN 1.0, we passed the IoT security baton to the internet community, so that we can focus more on domain name security and the secure internet of the future.



TimeNL

The Network Time Protocol (NTP) is the most widely used protocol for synchronising the clocks on computer systems. Stable and accurate timing is vital for all kinds of applications to function properly. For example, we need precise time stamps in order to ascertain who applied to register a domain name first. Reliable timing is also needed for attaching a digital signature to a domain in the context of DNSSEC.

In 2019, we introduced our own public time service, TimeNL, in order to highlight the importance of NTP and make the service's characteristics clear to users. TimeNL has proved a big success: our twenty-eight globally distributed servers now process about 100,000 NTP queries a second. Of those, about 10 per cent originate from the Netherlands.

In 2021, we added TimeNL to the NTP Pool, meaning that it is unconditionally available to everyone free of charge. We also use TimeNL within SIDN.

Our TimeNL service highlights the importance of NTP.

COMAR

COMAR (Classification of **CO**mpromised versus **MA**liciously **R**egistered Domains) is a joint research project run by SIDN Labs, French registry AFNIC and Grenoble Alps University. Its aim is to develop a system that can automatically distinguish between domain names registered by cybercriminals for malicious purposes, and legitimately registered domain names that are subsequently abused by exploiting vulnerabilities in web applications. A prototype of the software is now ready for use.

LogoMotive

Fraudsters often use the logos of well-known, authoritative organisations, such as government agencies and national institutes, to make their malicious websites look trustworthy. SIDN Labs has therefore developed a system called LogoMotive based on the well-established YOLO (You Only Look Once) algorithm. LogoMotive has been created to protect .nl users against internet crime. In 2021, the system was piloted with the Dutch government and a consumer trust mark scheme. As well as detecting phishing websites, the pilots revealed a number of legitimate government websites that the central administrators were unaware of.

LEMMINGS

If mail traffic continues after the cancellation of a domain name, and the name is subsequently re-registered by a new registrant, sensitive data may fall into the wrong hands. The Dutch police and various care establishments in the Netherlands have suffered data breaches under such circumstances. The automatic detection of potentially problematic situations can therefore help to prevent the loss of private information.

In 2021, SIDN Labs developed a system to do that: LEMMINGS (deLetEd doMain MaIl warNinG System). The prototype system works by analysing DNS traffic for evidence of mail addressed to cancelled domain names. The former registrants are then alerted by e-mail. Last year, we ran LEMMINGS pilots with two registrars, Argeweb and Openprovider. In the pilots, LEMMINGS sent a total of 870 warnings to former registrants, without causing extra work for the two registrars.



Moritz Müller
Research Engineer, SIDN Labs

29



Moritz awarded a doctorate *cum laude*

In 2021, Moritz Müller was awarded a doctorate *cum laude* by the University of Twente. He defended his thesis Making DNSSEC Future Proof on Friday 24 September. Moritz is a Research Engineer at SIDN Labs, our research team, which works to help the Dutch, European and global communities by contributing to ongoing improvement of the internet infrastructure's reliability. In his thesis, Moritz highlights the big challenges facing the DNS and DNSSEC on the internet of the near future. He also puts forward solutions for making DNSSEC more future-proof and improving the internet community's preparedness for protecting the DNS and DNSSEC against (future) threats. We are of course very proud of Moritz's achievements. > [Read more on sidnlabs.nl](https://sidnlabs.nl).



SIDN Fund

The internet has great benefits for society. It offers the potential for applications with huge economic and social value. However, dependency on the internet is also a source of vulnerability. Since 2015, SIDN Fund has therefore been working to promote a strong internet for everyone by supporting innovative internet projects. The Fund has now assisted more than three hundred projects. SIDN Fund has an independent Board of Governors and Executive Board.

SIDN Fund's activities are evaluated once every three years, and 2021 was one such year. One of the main findings was that the new programmatic approach adopted by the Fund in summer 2019 has been working well. It sharpens the focus and amplifies the impact by increasing coherence amongst themed projects. In future, therefore, the Fund will organise

open calls only for Pioneer Projects. The practice of scouting larger projects suitable for support, as with the [Dutch Security Report Portal](#) and [Baas in Eigen Bubbel](#) ('Be Boss of Your Bubble'), will also be continued.

By following that approach, SIDN Fund was again able to support numerous impactful projects on relevant themes in 2021. The Fund organises two open calls a year. In spring 2021, a themed call was also organised: proposals were invited for projects involving the development of tools and instruments for getting a grip on disinformation and its dissemination. Seven projects linked to that theme were ultimately awarded grants. SIDN Fund also addressed the issues of inclusion and digital access, organising a call on the theme of 'Inclusion and accessibility – Participating in the digital society'. The aim of the call was to further promote the accessibility and inclusivity of digital services, websites and apps, thus improving the position of people with disabilities and other vulnerable groups within our digital society. Nine projects linked to the theme were funded. Following the successful collaboration in 2020, a joint call was organised with the Eindhoven Cultural Foundation in November 2021, under the banner of 'Technician Seeks Designer 2021'. Its goal was to identify designers interested in using their expertise to help take a promising SIDN Fund-supported internet project to the next level. Eight matches were made to form collaborative teams. Applications for Pioneer Project funding of up to €10,000 can be made all year round. In 2021, a total of seventeen Pioneer Projects were awarded grants.

Fig. 11 | Annual contribution to SIDN Fund (€m)



Some of the projects supported by SIDN Fund in 2021

Mediajungle

Fake news, disinformation and false reports are nothing new. However, the rise of social media has greatly accelerated the spread of such problematic material. It has also become harder to distinguish truth from fiction. The Mediajungle team and their partners have therefore developed a series of tools, including a 'serious game' (a game with an educational purpose), videos and animations. The tools are designed to promote balanced dialogue about how the internet works, and the opportunities and risks it brings. Mediajungle focuses mainly on young people with mild mental disabilities, with the aim of making them less vulnerable to disinformation. The initiative therefore dovetailed neatly with the themed call 'Getting a grip on disinformation'.

Inaccessible App Reporting Portal

Many governmental and commercial apps and websites aren't suitable for use by people with impaired vision and other disabilities. The Appt Foundation has therefore teamed up with designers Simon Dogger and Hedwich Hooghiemstra to make apps more accessible for people with various forms of disability. They have launched the Inaccessible App Reporting Portal, where people with disabilities and their carers can report apps that offer poor access. The Appt Foundation processes the reports, then contacts the operators of the apps and websites in question and helps them understand how they can make their products more accessible. The project was funded through the open call 'Technician Seeks Designer'.



Bellingcat

It is vital that facts relating to wrongdoing are brought to light, so that global conflicts, crimes against humanity and other misdeeds can be understood and prevented. Bellingcat is an independent, international collective of investigators and citizen journalists dedicated to revealing facts online and in open-source form. With a view to further facilitating online citizen investigative journalism, Bellingcat has developed the Bellingcat Volunteer Hub: a platform for collaboration amongst volunteers and investigators. The Hub will promote open-source methods and extend the community of investigators working in the field. The project is providing innovative ways of tackling wrongdoing and social challenges, in line with SIDN Fund's goal of advancing 'Tech for Good'.

By supporting the Inaccessible App Reporting Portal, we are promoting online inclusion and accessibility.

Digikwis

Since the pandemic hit, video calling has become part and parcel of many people's lives. However, not everyone is able to use the software needed for video calling. DigiKwis is therefore developing free, low-threshold educational material and quizzes to show people how to use Zoom and Microsoft Teams. The goal of this Pioneer Project is to help people understand video calling and build digital self-confidence. The initiative ties in with SIDN Fund's user empowerment objective and contributes to improved digital accessibility and internet inclusivity. The lessons are freely available from the [DigiKwis website](#).

DataLekt

Cyber-incidents involving data breaches, ransomware and the like are increasingly commonplace. It's important to understand such incidents, how they occur and what their consequences are. Against that background, MITE3 Cybersecurity started the DataLekt project to provide information about all hacks, data breaches and other cyber-incidents involving Dutch organisations since 2016. The website datalekt.nl was set up for the project in October 2021. The website presents graphical data on the types of incident occurring and their frequency. Articles, quizzes and links to external information sources are also shared to provide organisations, citizens, students, researchers and cyber security specialists with the fullest possible picture. DataLekt supports SIDN Fund's user empowerment objective and helps to promote awareness and understanding of cyber-incidents, thus preventing more people falling victim.

Publicroam

In 2020, SIDN Fund joined forces with the Eindhoven Cultural Foundation to organise a call for proposals linked to the theme of 'Technician Seeks Designer'. The aim was to recruit designers interested in using their expertise to improve the user-friendliness and accessibility of projects with a technical focus, and thus boost their impact. A series of online sessions resulted in the matching up of eight teams of technicians and designers. All the projects have since started. One of the initiatives supported by SIDN Fund as part of the programme was Publicroam. The project involves creation of a secure, privacy-friendly Wi-Fi service for use in public buildings and facilities. After completing a free one-time registration process, a Publicroam user is automatically and securely connected to the internet via the Wi-Fi of any participating organisation. Designers at Kickoff Lab gave their support to the Publicroam project, improving the registration process and developing a communication kit for Publicroam location

Contributions to organisations and conferences

We play an active role in various important international forums. Our main involvements are outlined below. Due to the coronavirus crisis, most meetings took place online in 2021.

ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organisation that coordinates internet-related tasks. For example, ICANN is the forum within which policies governing



SIDN people were actively involved in the meetings and more generally within ICANN. For example, we are subscription-paying members of the ccNSO Strategic and Operational Planning Standing Committee, the Security Stability Advisory Committee (SSAC), the ccNSO PDP Working Group – which is working on a procedure for appealing against country-code delegation decisions made by the Internet Assigned Number Authority (IANA) – and the CSC Review Team. We also speak for the ccNSO in liaison with the GNSO Council.

At ICANN72, one of our colleagues made a presentation on DNSSEC disaster recovery. We also worked with the Ministry of Economic Affairs and Climate Policy to organise preparatory sessions for Dutch stakeholders ahead of each ICANN meeting.

RIPE

We have worked with RIPE for many years. RIPE is responsible for issuing IP addresses to internet service providers and other bodies in Europe, the Middle East and parts of Central Asia. One of our colleagues was made Co-chair of RIPE's DNS Working Group in 2021. There were two virtual RIPE meetings during the year. Our input included a presentation on the tsuNAME vulnerability by SIDN Labs.

IETF

The Internet Engineering Task Force (IETF) is an open, international community of network designers, operators, suppliers and researchers. The community works on evolution of the internet architecture and on improving internet performance. The three IETF meetings in 2021 were again held online. SIDN Labs was actively involved, giving presentations on various subjects, including tsuNAME.

CENTR

responsible for 80 per cent of all registered country-code domain names in the world. Each year, CENTR organises several workshops in the fields of marketing, security, administration, legislation and regulation, security, and research and development. In 2021, SIDN Labs made multiple presentations on topics including COMAR, Anteatser and the DDoS Clearing House.

At CENTR's AGM in March 2021, our CEO was appointed to CENTR's Board of Directors. The annual Registrar Day, to which we traditionally invite .nl registrars, took place in June. The event formed part of CENTR Members' Day, previously known as the CENTR Jamboree.

DNS-OARC

The DNS Operations, Analysis and Research Center (DNS-OARC) provides a reliable platform for key operators, analysts and researchers to share information and knowledge and coordinate responses to attacks and other problems. OARC 34, 35 and 36 took place in 2021, with various presentations by SIDN and SIDN Labs personnel.

ECP Annual Festival

In 2021, ECP | Platform for the Information Society organised a hybrid version of its Annual Festival. Delegates could attend in person at the Fokker Terminal in The Hague or participate virtually in the interactive programme of debates, sessions, workshops and networking opportunities. As usual, we were one of the event partners. In tandem with SIDN Fund, we delivered two sessions, one of them a joint session with TNO devoted to the ethical use of artificial intelligence: Responsible Deployment of Algorithms in Your Municipality. The other session was about disinformation and its threat to democracy, organised in collaboration with NL IGF.

EuroDIG

European Dialogue on Internet Governance (EuroDIG) is an open, multi-stakeholder platform for pan-European discussion of the internet and its governance. We're among the organisations that support the platform. EuroDIG allows all members to raise items for inclusion on the agenda. It is therefore the forum for debating issues without decision-making. The platform is intended primarily to enable as many stakeholders as possible to discuss internet governance, as a basis for building a stronger internet for all. EuroDIG 2021 took place online in June. It is hoped that EuroDIG 2022 can be held in Italy.



Internet Governance Forum

The Internet Governance Forum (IGF) is part of the United Nations and, like EuroDIG, is a forum for the discussion of internet governance issues, but at the global level. The IGF's annual meeting is attended by representatives of governments, market actors and citizens' organisations. The sixteenth edition was held in Poland in December. We contributed to various sessions.

ONE Conference

The ONE Conference is one of the biggest international gatherings in the field of cybersecurity. It is organised by the Ministry of Economic Affairs and Climate Policy, the NCSC and the Municipality of The Hague. The ONE Conference 2021 was held on 28 and 29 September, with SIDN Labs making a presentation on tsuNAME, a serious DNS vulnerability.

SIDN Inspire

Our own hybrid event, SIDN Inspire, was postponed from 2021 to Wednesday 25 May 2022. The venue will be the Media Plaza in Utrecht and the proceedings will be live-streamed. A key element of the programme will be the .nl domain's thirty-fifth anniversary. However, the event will mainly look ahead, in line with its theme: Future Internet.

Involvement with outside organisations

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

Internet Security Platform

The Internet Security Platform is a joint public-private initiative intended to promote internet security. The platform addresses issues such as phishing, privacy and how to tackle the distribution of child sexual exploitation material on the internet. In 2021, we were again active on the platform, participating in initiatives such as Veiliginternetten.nl, Internet.nl and e-mail security campaigns.

Notice-and-Take-Down Working Group

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

Online Child Abuse Expertise Bureau

We are one of the main financiers of the Online Child Abuse Expertise Bureau (OCAEB), which works to prevent and intervene against child sexual exploitation on the internet. The Bureau is affiliated to INHOPE, an international network of similar organisations.

Children safe on internet

Having been brought together by the then Minister of Justice and Security Ferdinand Grapperhaus, various public and private-sector actors, including SIDN, work together to tackle the online sexual exploitation of children. Participants cooperate on initiatives aimed at substantially reducing the use of Dutch servers for the distribution of child sexual exploitation material.

IDnext

IDnext is an open, independent platform that supports innovative approaches in the field of digital identities. Its aims are to generate awareness and to provide a knowledge and networking platform for experts in IT, business and marketing. We worked with the platform to organise the hybrid IDnext Event 2021, whose theme was the importance of digital identity.

Alert Online

Alert Online is intended to boost awareness of online security issues, to promote cybersecure behaviour and to increase related knowledge. Established by the Ministry of Economic Affairs and Climate Policy, the campaign is concerned with the cybersecurity of citizens, enterprises and government bodies. In 2021 we created content relating to topics such as phishing, ransomware and two-step verification.



Bits of Freedom

Bits of Freedom is a foundation that fights for privacy, freedom of communication and an internet that is open to all. Because its aims are closely aligned with our own mission, we are one of the Foundation's sponsors.

TUCCR

We are co-founders of the Twente University Centre for Cybersecurity Research (TUCCR), a joint venture dedicated to reinforcing the security and digital autonomy of our society by means of knowledge, innovation and the nurturing of talent. TUCCR was launched on 5 March 2021, with our CEO holding a seat on the Board of Directors.

DINL

Digital Infrastructure Netherlands (DINL) is a foundation that campaigns for a strong digital infrastructure as the foundation of the Dutch digital economy. We are one of the coalition's founding members. DINL represents the thousands of entities that deliver the facilities and basic online services underpinning the digital economy. It informs government bodies, companies and citizens about the digital economy and flags up opportunities to reinforce the Netherlands' status as an international, digital leader. In February 2021, a group of eight organisations, including DINL, joined forces to establish the Digital Parliamentary Academy. As a neutral, independent platform, ECP acts as the Academy's secretariat. The Digital Parliamentary Academy delivers knowledge and information sessions to communicate reliable, neutral information about the digital world to the political community. In May 2021, SIDN Fund CEO Valerie Frissen delivered a session entitled 'Data as the citizen's property'.

ECP

We partner ECP, a neutral platform for the digital society that works to promote a resilient, opportunity-rich digital society in which everyone can participate. Within the ECP, members of the scientific and business communities, government agencies and community organisations all work together and exchange knowledge about how to shape a responsible digital society.

NLnet Labs

NLnet Labs is an R&D institute that develops open-source software for the core of the internet. The institute has a global reputation for its work on the DNS, DNSSEC and RPKI. NLnet Labs' DNS software is used on millions of servers all over the world. We sponsor some of NLnet Labs' activities. In addition, SIDN Labs works closely with the institute on various research projects, such as the CATRIN Responsible Internet project.

Summer School on Internet Governance

We sponsor the annual European Summer School on Internet Governance (EuroSSIG), a comprehensive introduction to the topic of internet governance aimed at students, academics, civil servants and businesspeople. The fifteenth EuroSSIG was held in Meißen in August 2021.

Dutch Cloud Community

In January 2021, the Dutch Cloud Community was formed by the merger of ISPCoconnect and DHPA, the sector's two trade associations. More than a hundred prominent companies are affiliated to DCC, which therefore serves as the voice of the digital infrastructure. ISPCoconnect and the DHPA were behind creation of the DINL Foundation, of which we are co-founders. We sponsor the DCC's efforts to promote an open, secure and free internet.

Dutch Anti-DDoS Coalition

The National Anti-DDoS Coalition exists to increase the Netherlands' resilience to DDoS attacks. The Coalition has seventeen member organisations from various sectors. We are one of the members, and the others include government agencies, internet access providers, internet exchanges, academic centres, non-profit organisations and banks. The Coalition will ultimately make use of the DDoS Clearing House that we are developing within CONCORDIA.

CONCORDIA

SIDN Labs is a member of CONCORDIA, a European consortium that investigates new cybersecurity mechanisms and applications. Within the consortium, SIDN Labs focuses on development and



evaluation of the DDoS Clearing House and running pilots. The DDoS Clearing House is a system that enables anti-DDoS coalitions, such as the Dutch national coalition, to exchange data on DDoS attacks and thus improve their members' preparedness. The CONCORDIA project started on 1 January 2019 and is set to continue until 1 January 2023.

2STiC

In 2019, SIDN Labs and several partners started a research programme called Security, Stability and Transparency in inter-network Communication, or 2STiC for short. The 2STiC consortium is developing and evaluating mechanisms for increasing the security, stability and transparency of internet communications. Its members are working both on extensions to the existing internet and on emerging internet architectures, such as SCION, RINA and NDN.

Abuse Information Exchange

We are one of the organisations behind the Abuse Information Exchange, whose members are internet access providers representing more than 90 per cent of the Dutch market. Members exchange information about botnets and other forms of internet abuse in the Netherlands, with a view to improving the speed and quality of the response.

Liaison with the NCSC

The National Cyber Security Centre (NCSC) is part of the Ministry of Justice and Security, which works with partners to promote internet security. We act as the link between the National Cyber Security Centre (NCSC) and the other partner organisations. We also share knowledge and information with the NCSC.

ACCSS

ACCSS (ACademic Cyber Security Society) is a society for art, science and social science academics in the Netherlands who are active in the field of cybersecurity. In 2021, we sponsored the Society's establishment. One of our colleagues was recently appointed to the ACCSS Advisory Panel.

Outlook

SIDN Labs

LogoMotive

In 2022, we plan to integrate LogoMotive into SIDN BrandGuard. BrandGuard users will then be able to scan the internet for sites making unauthorised use of their logos. With this initiative, we are aiming to give brand owners and internet users better protection against fraud and brand abuse. We also intend to publish a peer-reviewed paper on the pilots we ran in 2021 and make our source code available to other researchers and registries. The dataset being compiled by SIDN BrandGuard will be used for further research and refinement of the system.

DDoS Clearing House pilot

In 2022, we will run a pilot with the DDoS Clearing House. The project will involve scaling up the testbed we developed in 2021 and will enable National Anti-DDoS Coalition members to evaluate how the Clearing House works in practice. The pilot's findings will serve as input for CONCORDIA. After the pilot, the National Internet Providers Management Organization (NBIP) will operate the production version of the DDoS Clearing House for the National Anti-DDoS Coalition.

Reliable internet infrastructure

We plan to set up an abuse detection pilot with other DNS operators, involving the use of federated learning to develop a joint machine-learning model for phishing site detection. We will also perform measurements designed to shed more light on the security and evolution of the internet. In 2022, our LEMMINGS system will be rolled out to all .nl registrars, so that all .nl domain names are protected. We will also integrate COMAR into the tools used by our support team.

The Responsible Internet

We are developing an attractive demonstrator of a more transparent network infrastructure, with a view to generating interest from prospective pilot partners, for example. Finally, in the interests of knowledge-sharing, we plan to organise an international workshop on the infrastructure of the Responsible Internet.

SIDN Fund

In light of the evaluation of SIDN Fund's work between 2018 and 2020, it was decided that we should continue financing the Fund in the coming years. The Fund will continue the themed call strategy. SIDN Fund will also seek to strengthen



strategic collaboration with actors capable of securing impact. Such actors include organisations focusing on continued development projects or practical applications. In spring 2022, the Fund will be calling for proposals linked to the theme of disinformation. In 2022, we intend to reinforce collaboration between SIDN Labs and SIDN Fund, with a view to addressing major internet-related problems affecting our digital infrastructure. SIDN Labs will concentrate mainly on the internet infrastructure, while SIDN Fund tackles end-user issues. Finally, in the year ahead, SIDN Fund will be looking to raise the profile of its activities and impact, particularly in the context of the public debate regarding a secure, open and trustworthy internet. To that end, the Fund will be increasing its result-sharing and communication activities, and placing greater emphasis on telling its story, for example.



Karien Sondervan
Director, CyberSoek

37

Promoting digital self-sufficiency

More than 20 per cent of Dutch people have difficulty with modern digital technology. Helping such people depends on bespoke intervention. CyberSoek is an Amsterdam-based initiative dedicated to promoting digital self-sufficiency. The organisation has been pursuing its goal of universal digital inclusion for twenty years by offering free coaching. CyberSoek's Director, Karien Sondervan: "We've developed a unique, innovative method, and we share our expertise with partners in Amsterdam and beyond. In 2021, we received a grant from SIDN Fund to cover the cost of upgrading our Train the Trainer course and creating a website, manual and instruction videos. We'll be making the package available to 130 partners working in the field. The Fund's support is also enabling us to draw up a plan for upscaling and a nationwide rollout."

> [Read more on cybersoek.nl](https://cybersoek.nl).



04

Milestones, partnerships and team progression

Internal developments

The defining theme of 2021 was the .nl domain's thirty-fifth anniversary. It was also the year that SIDN Labs celebrated its tenth anniversary. Unfortunately, the coronavirus pandemic continued to impact our working and personal lives. We nevertheless welcomed numerous new team members and started on the development and introduction of a hybrid working concept. In order to stay in contact with each other and to receive and coach new colleagues, we organised frequent online activities.



04

Milestones, partnerships and team progression

Internal developments

At SIDN, we seek to maximise the value we create for the community and economy of the Netherlands. We are proud to bear the responsibility of a key public role and a significant influence on society.

We are a true knowledge organisation, working every day to create a better, securer internet. Many of our people are highly educated and possess specialist knowledge. We facilitate the development and progression of our people by investing in education and training. And, as befits the rapidly changing world in which we operate, we are constantly adapting the way we work. Enabling us to respond more quickly and effectively to the changing expectations of our customers, the internet and the wider community.

Crowning moment of a jubilee year

Although the pandemic prevented us marking .nl's thirty-fifth anniversary and SIDN's twenty-fifth with a physical celebration, we took great pleasure in looking back at all that has been achieved. At how today's secure and stable internet infrastructure was built from the ground up. The crowning moment of our jubilee year came on Tuesday 16 November, when King Willem-Alexander paid us a virtual working visit. He spoke to a number of our people and stakeholders about the history of SIDN, development of the .nl domain, the future of the internet, and the work being done to maintain the security of .nl for all its users. The entire SIDN workforce watched the visit live.

> [Watch a compilation video of the visit.](#)

Home and hybrid working

In 2020, our technical resources and flexibility enabled us to take the switch to home working comfortably in our stride. After a year of working almost exclusively from home, we started development of a hybrid working concept in 2021. The aim of the concept is to enable us to secure the best of both home working and office working.

We want to retain the benefits of home working, such as reduced commuting and CO₂ emissions, and more focused and therefore more productive workers. That implies the office taking on a modified role as a place to meet, a place where people collaborate, brainstorm and exchange ideas. The year started with development of a vision of hybrid working. We envisaged a scenario where, within certain parameters defined at the organisational level, our people are free to choose where they work. Detailed operational arrangements would then be made at the team level. We installed video conferencing equipment in all the conference rooms at our office complex, while also providing personnel with the equipment needed to set up home workstations.

The king's visit was the crowning moment of our jubilee year.

Workforce and sickness absence

Because social and economic digitisation was greatly accelerated everywhere by the pandemic, people with ICT skills were in great demand. We had a number of ICT vacancies last year, as a result of both staff turnover and the expansion of our activities. We therefore deployed additional ICT recruiters to fill the vacancies. Against that backdrop, seventeen new recruits joined us in 2021. The onboarding and acclimatisation programme developed in 2020 was therefore put to good use. An identical number of our colleagues moved on during the year. Hence, we ended the year with a workforce of 109 (99.2 FTEs). While the national average absence rate rose to 4.8 per cent, ours fell to 2.3 per cent.



Training and development

With the aim of giving our staff more control over their development, in 2021 we implemented a new platform for performance management called Dialog. As in previous years, we promoted staff development by reserving 7 per cent of the wage bill for training. Although e-learning is increasingly commonplace, fewer people took training in 2021 than prior to the pandemic.

Seventeen of our colleagues opted for a new challenge, while an identical number of newcomers joined us.

Procedures

In 2021, we worked increasingly in line with the DevOps method, where the emphasis is on collaboration and communication between software engineers and ICT specialists. We also placed greater emphasis on the use of Agile and Scrum teams throughout the organisation and made use of CI/CD pipelines. The approach has been adopted from the world of software development, where code modifications involve a number of automated steps. We also separated the infrastructure and development side of our ICT team, with a manager for each unit, so that staff receive additional guidance. The aim of the changes is to make the organisation more agile and able to respond to developments in the outside world. The wishes of our customers, the internet users, and the welfare of our personnel are always our primary concerns.

Internal systems

Our CRM system was upgraded in 2021 to make it more dynamic. We switched to a new system that is better aligned with the needs of Sales and Finance and we automated many internal processes. We also introduced two-factor authentication for all our business systems, as an additional layer of security for the web interface of the Domain Registration System (DRS).

Personal sponsorship budgets

One feature of the wide package of benefits given to our personnel is a personal sponsorship budget: a sum of money that the individual can donate to a good cause of their choice. This year, many of our colleagues chose to support the jubilee appeal organised by Piet Beertema. As part of the

activities linked to .nl's thirty-fifth anniversary, he invited donations to Free a Girl: a globally active Dutch charity dedicated to rescuing under-age girls from prostitution and pursuing the people who exploit them. A generous sum of €57,000 was raised. Another popular charity was Trees for All. As soon as pandemic-related restrictions allow, we will be working with Trees for All to create an SIDN wood with at least 2,583 trees. The first trees in our 'company woods' will be planted by our own personnel.

Sustainability

Planting trees is by no means our only contribution to sustainability. In 2021, we defined a number of Sustainable Development Goals, on the basis of which we developed a Climate Plan. The plan sets out our ideas on socially responsible procurement and operations, energy conservation and the use of green energy. We also took practical steps towards reducing our carbon footprint in 2021. We replaced the solar panels on the roof of our office block with a larger, more modern array. The new panels are manufactured on a CO₂-neutral basis and supply twice as much power as the old ones. The old panels were sold for reuse. Extra EV charging points and a sustainable water management system were installed as well.

We're working with Trees for All to plant 2,583 trees in our own 'company woods'.

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 2021, we successfully secured renewal for an eleventh year. We also standardised many of our information processes.

Privacy Board

Since 2014, we've had an internal Privacy Board that reviews privacy policies developed by colleagues. A privacy policy is prepared for anything that involves the processing of privacy-sensitive data, explaining how and why the data is processed. In 2021, we published four policies and the associated assessments, including documents for JITTER. JITTER is a prototype system developed by SIDN Labs, which uses machine learning to generate



Crowning moment of a jubilee year

For us, 2021 was a year of anniversaries: thirty-five years of .nl, twenty-five years of SIDN and ten years of SIDN Labs. The crowning moment of our jubilee year came on Tuesday 16 November, when King Willem-Alexander paid us a virtual working visit. He spoke to a number of our people and stakeholders about the history of SIDN, development of the .nl domain, the future of the internet, and the work being done to maintain the security of .nl for all its users. The entire SIDN workforce watched the visit live.

> [Watch a compilation video of the visit.](#)



warnings regarding suspect domain names potentially usable for malicious content. The system facilitates the identification of abuse before the relevant domain names appear in abuse lists.

All privacy policies and the associated Privacy Board assessments are published on our website.

> For details, see sidn.nl.

Staff Council

Our Staff Council was asked to approve multiple proposals, regarding matters such as the new privacy statement, the introduction of an expenses claim tool and performance management tool, and the replacement of our payroll system and HR software. A meeting between the Council and SIDN's Supervisory Board took place in September.

Collaboration with universities and colleges

In 2022, we will take part in the 'Make IT Work' programme, partnering with the HAN University of Applied Sciences and others. The programme offers higher vocational retraining for IT roles. Students begin by taking a full-time software engineering course at HAN, after which we provide further training. Phase 1 has already begun, and the first three participants are due to start at SIDN in July 2022. By reaching out to and working with universities, colleges and new IT professionals, we aim to continue raising our profile on the labour market.

Outlook for 2022

Hybrid working

We will continue working from home much of the time, at least in the early part of 2022. However, hybrid working will remain an important theme. We intend to improve and roll out our new hybrid working method, with continued emphasis on collaboration, connection and good internal communication. We will also give our colleagues opportunity to find a good balance within the new structure.

Diversity and inclusion

In the year ahead, we plan to refine our vision of a diverse and inclusive workforce. We believe it is important to define clear diversity and inclusivity goals and plans for achieving them.

Training and development

We will continue to help our colleagues achieve personal development goals. Over the next twelve months, we will extend the performance management tool introduced in 2021. A learning platform will be added, on which learning resources will be made available and learning pathways set out.

Sustainability

In 2022, we will start work on realisation of the ambitions set out in our Climate Plan, which runs until 2025. Care will be taken to ensure that our activities are aligned with the National Climate Agreement.



Yvette van Room
Facilities Officer, SIDN

Preparing for hybrid working

In 2021, we started the development of a hybrid working concept. The aim is to secure the best of both home working and office working. We want to retain the benefits of home working, such as reduced commuting and CO2 emissions, and more focused and therefore more productive workers. SIDN's Facilities Officer Yvette van Room: "Our office building serves increasingly as a meeting place – a place where people collaborate, brainstorm and exchange ideas.

We've installed video conferencing equipment in all our conference rooms, and we've made sure that all meetings can be organised on a hybrid basis. We're also working on a system of flexible individual workstations and creating comfortable, atmospheric meeting places."

> [Read more on page 39.](#)



05

Supervisory Board



“SIDN continues to do important visible and invisible work for a stable and strong .nl domain and a safer internet.”

Paul Schnabel
Chair, SIDN Supervisory Board

45

SIDN continues to do important visible and invisible work

2021 was another extraordinary year. A year of highs, such as our anniversary celebrations and the virtual royal visit... and lows, such as the ongoing restrictions on face-to-face gatherings. Although the organisation took the switch to home working in its stride, both the staff and the Supervisory Board missed the opportunities to exchange ideas, views and knowledge in person and celebrate important occasions together. SIDN continues to play an extremely influential role. A role that has been vital during the coronavirus crisis, but will remain no less important going forward. SIDN continues to do important visible and invisible work for a stable and strong .nl domain and a safer internet.

In 2021, the Supervisory Board occasionally met physically, but most meetings took place online. Pandemic-related restrictions meant that no face-to-face meetings with outside parties were held. On 16 November, however, we were able to welcome a very special guest to SIDN: King Willem-Alexander. At the start of his virtual working visit, the King spoke with us about the history and development of the .nl domain, what we're doing to make sure .nl remains one of the world's most secure domains, and how we assure its continuous availability. For us, the visit was the crowning moment of the .nl domain's thirty-fifth anniversary year.

In 2021, the Supervisory Board said farewell to Willem van Waveren and Peter van Schelven, both of whom had made key contributions to our work. Peter was succeeded by Lokke Moerel, who joined the Board at the end of 2020. We were also strengthened by the arrival of Gerben van Leeuwen and Dennis Raithel. Gerben was proposed by the Registrars' Association (RA) and



has many years' experience as a registrar. He was the owner-proprietor of Argeweb, Amsio and SaasNow, for example, and now sits on the DINL Board. He is also co-founder and owner of X-Corp B.V. As well as being a member of our Supervisory Board, Dennis sits on SIDN Fund's Board of Governors and Audit Committee. In addition, he has a seat on the BDO Supervisory Board and the Board of STEDO, chairs the BDO Audit Committee and acts as an advisor to the Supervisory Board of Hydratec Industries. For the moment, our Supervisory Board has eight members.

At SIDN, monitoring developments within the organisation and its environment remains an important task. Last year, the Supervisory Board therefore critically reviewed SIDN's strategic plan, its product development activities and utilisation of new opportunities. We also took a close look at the main action points identified by the Registrar Satisfaction Survey. Such activities enable us to maintain a clear view of our position in the field and how customers feel about our services. On 1 January 2021, SIDN and the RA signed a new cooperation agreement, under which both parties committed themselves to constructive dialogue and coordination between the registrar community and SIDN on registry activities. The new agreement is based on the principle of mutual respect for one another's independence.

In 2021, SIDN worked in many different ways to promote problem-free, opportunity-rich digital living for everyone. For example, SIDN Labs was active in the field of fake webshop detection and closure. Through SIDN Fund, we also supported efforts to tackle the distribution of child sexual exploitation material. In the field of cybersecurity and online identities, we made considerable strides, including progress with the IRMA identification and authentication platform. The year ahead will be very important for IRMA. While we wait for the Digital Government Act to come into effect, we will continue to refine the technology. We regard making the internet and its infrastructure more secure and safeguarding citizens' privacy as public responsibilities, in relation to which IRMA can play an important role. We hope that the philosophy on which IRMA is based will be adopted in the upcoming legislation and by the European Commission in its planning for a European digital identity.

In 2021, the stability and health of SIDN and the strength of the .nl domain were again evident. At home and on the international stage, SIDN is held in high esteem. With a history stretching back thirty-five years, .nl is acknowledged as one of the oldest and biggest country-code domains in the world. We are also proud of the conspicuous progress taking place at SIDN Labs, which now has a team of twelve experts. In the space of just ten years, SIDN Labs has gone from a weblog to an influential centre for applied technical research in the field of internet security. Meanwhile, SIDN Fund continues to justify our enthusiastic support.

Paul Schnabel,
Chair of the Supervisory Board

About the Supervisory Board

The Supervisory Board oversees the work of SIDN's Chief Executive and the general situation within the organisation. The Board also supports the CEO with advice. The Supervisory Board considers matters such as SIDN's business strategy and the associated risks, realisation of the organisation's objectives and the design and effectiveness of the internal risk management and control systems. Topics addressed in 2021 included the transfer of CyberSterk to one of our partners in the service, SIDN's involvement with IRMA, cooperation with the RA, the evaluation of SIDN Fund and the (re-)appointment of new members to the Supervisory Board and its various committees. The Board also held regular discussions with the CEO regarding the organisation's performance during the lockdowns and regarding personnel welfare. In 2021, the SB carried out a self-evaluation.

Meetings

In 2021, the Supervisory Board held four virtual, face-to-face and hybrid routine meetings and one strategy meeting. September's routine meeting included a virtual discussion between the Supervisory Board and SIDN's Staff Council. Between the meetings, the Supervisory Board had regular contact with the CEO, and the Board's various committees (the Audit Committee, Selection and Appointments Committee and Security and Stability Committee) each met at least once.

The following were approved or adopted:

- SIDN's Annual Report and Annual Financial Statement for 2020
- 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 2022
- Proposals regarding decisions to be taken by SIDN in its capacity as shareholder in SIDN Deelnemingen B.V. and SIDN Business B.V., such as adoption of the Annual Financial Statement for 2020

Membership

The Supervisory Board has eight members. Gerben van Leeuwen joined the Supervisory Board in April 2021, and Dennis Raithela at the end of 2021.

Paul Schnabel, *Chair, Selection and Appointments Committee and Remuneration Committee*

Mark Frequin, *Selection and Appointments Committee and Remuneration Committee*

Simon Hania, *Security and Stability Committee*

Gerben van Leeuwen (appointed in April)

Lokke Moerel, *Security and Stability Committee*

Kees Neggers, *Security and Stability Committee*

Jeannine Peek, *Audit Committee*

Dennis Raithel, *Audit Committee, SIDN Fund Board of Governors* (appointed in November)

Peter van Schelven, *Audit Committee* (retired in March)

Willem van Waveren, *Audit Committee, SIDN Fund Board of Governors* (retired in April)

Supervisory Board Members' Retirement and Reappointment Rota

In accordance with Article 29 of its constitution, SIDN operates a rota for the retirement and reappointment of Supervisory Board members. The rota is summarised below.

	Appointment	Reappointment (where relevant)	Second reappointment (where relevant)	Expire date of current term of office	Term of last appointment
Paul Schnabel	September 2013	September 2016	September 2019	August 2022	Last appointment (-2022)
Simon Hania	April 2013	March 2016	April 2019	March 2022	Last appointment (-2022)
Kees Neggers	April 2014	March 2017	April 2020	March 2023	Last appointment (-2023)
Mark Frequin	April 2015	March 2018	April 2021	Maart 2024	Last appointment (-2024)
Jeannine Peek	July 2015	June 2018	July 2021	June 2024	Last appointment (-2024)
Lokke Moerel	December 2020	November 2023		November 2023	2026-2029
Gerben van Leeuwen*	April 2021	March 2024		March 2024	2027-2030
Dennis Raithel	November 2021	October 2024		October 2024	2027-2030

* Gerben van Leeuwen was appointed following proposal by the Registrars' Association (RA). In accordance with Article 24, clause 3C, of SIDN's statutes, the RA is to be asked for advice before the SB takes any decision regarding Mr Van Leeuwen's reappointment. Article 24, clause 3A and 3B, states that, before Gerben van Leeuwen's final term of office ends, the RA is to be asked to propose a successor or to advise on the appointment of a successor nominated by the SB.



o6

Annual Financial Statement



Notes to the Annual Financial Statement

In 2021, we recorded a negative result before taxes of €0.1 million. That is better than forecast, reflecting higher net turnover and lower operating costs. Net growth in the number of .nl domain names was also higher than forecast in 2021, due to organisations moving activities online in the face of continuing pandemic-related restrictions. In the budget for 2021, we made allowance for such restrictions limiting travel and other activities for several months of the year. In practice, however, the great majority of our events and outside event participations took place online. Furthermore, the progress of a number of projects, such as further development of the SIDN Academy, was slower than planned. As a result, operating costs were lower than initially budgeted.

Comparison with the previous year

In 2021, the operating result before taxes was a negative of €0.1 million, compared with a negative of €3.0 million in 2020. The number of .nl domain names increased by more than 120,000, to stand at more than 6.2 million by the end of 2021. The growth increased our net turnover. In 2021, we paid a total of €3.4 million to .nl registrars in the form of discounts and incentive payments – €0.2 million more than in 2020.

Operating costs were €20.6 million. That is €2.3 million lower than in 2020. The fall is the net result of increased expenditure on agency staff and a smaller donation to SIDN Fund. Agency staff were required for a large part of 2021 in order to cover unfilled vacancies. We also scaled up our ICT and recruitment capacities. Following the sale of our interest in Connectis at the start of April 2020, the associated goodwill has now been entirely written off. Hence, there will be no further goodwill depreciation charges. The increased expenditure on consultancy services in 2020 related entirely to the sale of Connectis. Expenditure on marketing and consequently overall costs were lower as a result of the transfer of CyberSterk to Guardian360 at the end of March 2021.

Taxes

In 2021, the simple operating result before taxes was a positive of €1.0 million, compared with a negative of €0.7 million in 2020. As a result, the corporation tax liability in respect of 2021 was €0.3 million higher than in 2020. At the start of 2022, a revised corporation tax declaration for 2020 was submitted. In the revised declaration, the additional contribution to SIDN Fund made in 2020 was treated as entirely non-tax-deductible. The effect was to increase the 2021 corporation tax liability by €0.5 million.

Financial strategy

The primary aim of our financial strategy is to assure the continuity of our services. That aim is translated into a solvency of at least 60 per cent and a contingency buffer equal to at least one year's expenditure. At the close of 2021, both our solvency and our equity capital were at target levels. Our treasury policy

is designed to mitigate liquidity risks. To that end, our liquid assets are spread across three Dutch banks. Since 2017, we have additionally held a portfolio of Dutch and German government bonds. The value of the holding is gradually decreasing as the bonds mature.

Breakdown of expenditure by strategy

In line with our desire to secure a responsible, positive return, we keep a critical eye on our expenditure. The expenditure associated with each of our strategies in 2021 is analysed below.

1. A valuable and value-based domain

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

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

With effect from 2021, corporation tax is no longer treated as expenditure. Moreover, the costs incurred by SIDN Labs in connection with .nl are accounted for under strategy 1. The interest payable on the loan that SIDN made to SIDN Deelnemingen BV is also attributed entirely to strategy 1. The comparable figures for 2020 have been adjusted accordingly.

2. Impact in two domains: online identity and cybersecurity

This heading covers expenditure on IRMAconnect, CyberSterk (ended at the start of April 2021) SIDN BrandGuard (previously the Domain Name Surveillance Service) and Connectis (interest sold at the start of April 2020).

3. Profit with a purpose

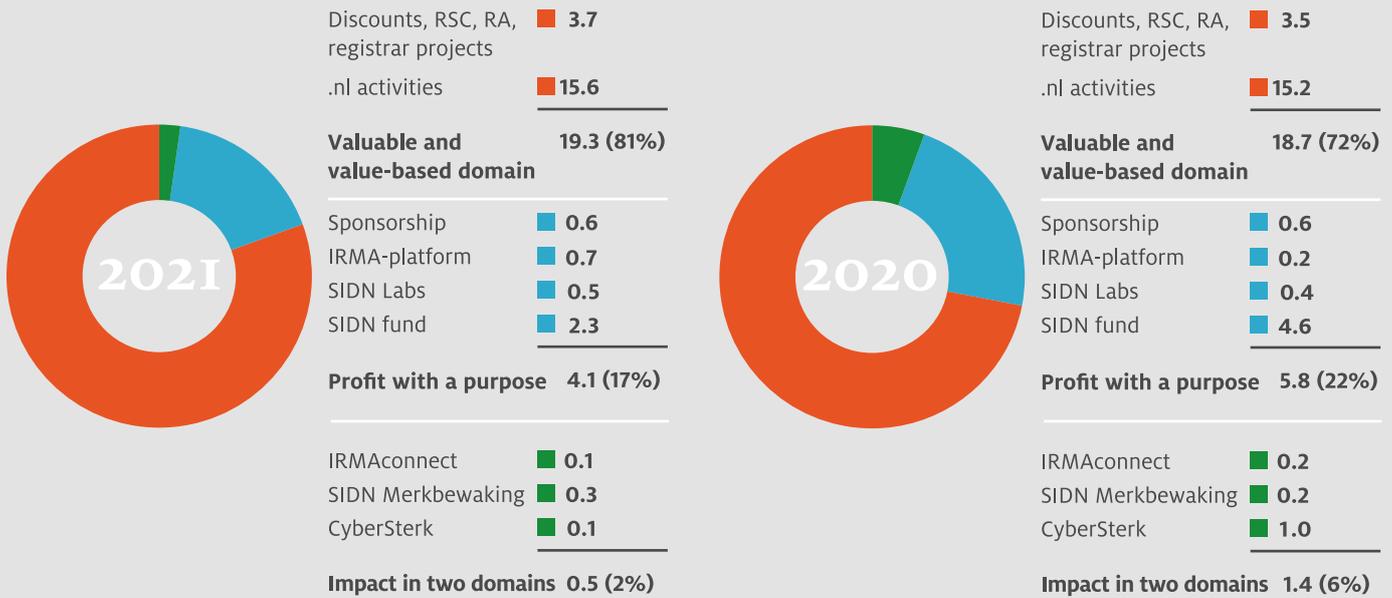
The positive return on the operation of .nl and our other activities is used for the benefit of the Dutch and international internet communities. This heading covers expenditure in that context, namely our funding of SIDN Fund, SIDN Labs and partners, the IRMA platform and community, and our sponsorship. Supported organisations include NLnet Labs (€225,000), ECP (€100,000), the Academic Cyber Security Society (ACSS) (€100,000), the Reporting Hotline for Internet Child Pornography (€60,000), IDnext (€40,000), Bits of Freedom (€40,000) and DINL (€20,000).

Actual expenditure per strategy, 2021 versus 2020

Total expenditure in 2021 was €2.0 million lower than in 2020. The fall was due to a smaller donation to SIDN Fund and the transfer of CyberSterk, after which all CyberSterk-related activities ceased. Expenditure on 'A valuable and value-based .nl domain' was higher, due to increased agency staff costs and discounts. We also continued our investment in the IRMA platform in 2021. IRMA-related investment will increase further in 2022, due to the cost of making IRMA fully compliant with (European) legislation and regulations.



Fig. 12 | Actual expenditure per strategy, detailed breakdown (€m)



Outlook

The coronavirus pandemic had major implications for all organisations. SIDN was no exception, experiencing both positive and negative impacts. The shift from physical activities to online activities was financially advantageous to us. However, the very limited scope for scheduled and ad hoc face-to-face meetings meant that many innovations and project-based activities were delayed and ran over to 2022. We attach particular importance to the welfare of our personnel – a subject that has our ongoing attention. We accordingly provide equipment for home working and ensure that any face-to-face meetings that do take place comply with the applicable guidance and are as safe as possible. We will invest further in our home working and office environments, in order to facilitate hybrid working.

In the years ahead, we expect net turnover to increase slightly, driven primarily by registration fee indexation and reduction of the direct debit discount from 5 to 2.5 per cent with effect from 1 January 2022. We are also investing in our ICT infrastructure, equipment and software, and in our working methods, with a view to increasing our agility and flexibility. We also continue to encourage our personnel to follow both further training courses and retraining courses, the scope for which has been curtailed for the last two years. Another ongoing field of investment is the security of both our internal computer systems and our services. The tight labour market obliges us to look at alternative approaches to recruitment and training. We are actively seeking collaborations and making more use of our contact network. Given the challenging labour market, the desire to maintain a flexible workforce and other factors, we seek to maintain a balance between permanent and temporary staff. That approach enables us to engage personnel with certain specialist expertise for periods of various lengths.

In 2022, we will carry forward development of the IRMA app, to ensure that it is fully compliant with the Digital Government Act. We will also add new functionalities and services to SIDN BrandGuard, with a view to increasing the service's added value.

Risk management

Vision

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

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

Governance and organisation

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

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

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

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



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

Risks and risk tolerance

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

Dealing with risks

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

Main risks and uncertainties

The main risks and uncertainties associated with our operations are identified below. The developments and control activities associated with each risk area during the year are also summarised.

51 Strategic risks

The main risks associated with SIDN's strategy stem from the strong dependence on (earnings from) the .nl domain and from the contraction of the .nl market. Our .nl domain registration services are sold through registrars. Through the Registrars' Association (RA), we therefore work closely with the registrar community on the promotion of .nl domain names and on continuous improvement of the security and quality of .nl. To that end, we entered into a new cooperation agreement with the RA at the end of 2020, which was extended at the end of 2021.

As a consequence of pandemic-related restrictions, we saw further growth in online service provision and .nl registrations in 2021. However, the pandemic's effects on the economy are likely to become apparent in the years ahead. Those effects will inevitably influence development of the .nl domain. In the years ahead, we expect the .nl market to remain stable. Given our limited capacity to influence the end market, our strategic risk tolerance is moderate.

We are seeking to increase our added value and extend the range of services we offer. As part of our strategy of achieving impact in the domains of online identity and cybersecurity, we have decided to continue investing in IRMA and SIDN BrandGuard.

Operating risks

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

Since 2011, we have been ISO27001-certified. In the context of our Information Security Management System (ISMS), we perform business impact analyses. That involves following an annual cycle in accordance with a defined information security policy. We also identify risks, implement control measures and assess residual risks. The findings, reports and internal and external audits are regularly discussed, e.g. in our Tactical Security Meetings, after which any necessary improvements are implemented. The outcomes are monitored by means of

Fig. 13 | SIDN's risk tolerance

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



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.

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

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

Financial risks

- *Solvency*
Solvency is equity capital expressed as a percentage of the balance sheet total. Between the close of 2020 and the close of 2021, solvency fell from 65.9 per cent to 62.9 per cent. The drop mainly reflects our increased levels of activity and the donations to SIDN Fund outstanding at the end of the year. The closing solvency figure at the close of 2021 remains above the defined minimum of 60 per cent.
- *Liquidity risk (including concentration risk)*
Liquidity risk is the risk of having insufficient liquid assets to meet our obligations. The balance of our liquid assets at the end of 2021 was €30.8 million, up €3.0 million on the close of 2020, due to repayment of the loan extended to Connectis. In recent years, our liquid assets have been buoyed by improved cash flow supported by increasing use of annual registration periods for .nl domain names. Our liquid asset balance is amply sufficient to cover our annual expenditure. Concentration risk is addressed by having our liquid assets spread across three Dutch banks.
- *Market risk*
Market risk is the risk of our government bonds and/or other securities decreasing in value. Our portfolio of Dutch and German government bonds was acquired with a view to holding the bonds until maturity. If circumstances should necessitate disposal of the bonds prior to maturity, we would face the risk of the bonds having lost some of their purchase value. Our holdings of other securities are at risk of declining in value. However, we have not detected any signs (trigger events) indicative of such an eventuality.
- *Currency risk*
Currency risk derives firstly from the risk that our other

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

- *Interest rate risk*
Interest rate risk is the risk that our government bonds and/or receivable loans are devalued by movement in market interest rates. Because we intend to hold our government bonds until maturity, the associated interest rate risk is small.
- *Credit risk*
Credit risk is the risk that a party with whom we have a contract defaults on their contractual obligations, as associated with other securities, accounts receivable, other receivables and liquid assets. Our bad debt risk is modest, because about 75 per cent of registrars pay by direct debit. Our General Terms and Conditions make provision for action to be taken if a registrar does not fulfil its financial obligations. Our policy is to distribute our liquid assets across three Dutch banks, thus mitigating the associated credit risk.
- *Damage claims and penalties*
This is the risk arising from service interruptions and data confidentiality or integrity breaches. Our General Terms and Conditions limit or exclude our liability for such problems. Our financial risk tolerance is moderate to low.

Legislative and regulatory risks

Changes to national or international legislation and regulations have the potential to affect our organisation and operating processes. We take stock of potentially significant proposed or impending legislative and regulatory changes – e.g. changes in employment law, tax law or data protection law – at an early stage. The impact of any such change is assessed and translated into organisational adaptations, which are then implemented. In view of the potential impact of legislative or regulatory changes relating to our registry role, we have appointed a Legal and 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. We amended our working practices where appropriate, and we voluntarily appointed a Data Protection Officer.

Since 2018, SIDN has been designated an operator of essential services under the Network and Information Systems Security Act. As such, we are subject to supervision by the Radiocommunications Agency, with which we regularly liaise.



The Agency is concerned specifically with the information security of our .nl services, in connection with which it performs audits. In 2021, the Agency carried out a follow-up audit. With the exception of a few action points, no matters of concern were identified. As well as being subject to audits, we are required to inform the NCSC and the regulator of any serious incidents, and we have a statutory duty of care, which covers risk control and incident prevention and mitigation.

Reputation risk

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

Contingency buffer

In order to assure the continuity of our organisation, it is important that we have an adequate financial buffer to protect against the possibility of losing a large portion of our income. The contingency buffer additionally serves to protect against the financial implications of the materialisation of an identified risk. Moreover, in the event of discontinuation, we would require sufficient funds to ensure the orderly winding up and/or transfer of our .nl activities.

53

Since recalibration in 2020, our minimum equity capital requirement is a sum equal to our annual expenditure. Our equity capital is currently above the defined minimum. Our Finance Department monitors the sufficiency of our equity capital in relation to the defined minimum and periodically reports its findings.



Consolidated financial statements for 2021

Consolidated balance sheet as at 31 December 2021 (after appropriation of profit)

	31 December 2021 (in €)	31 December 2020 (in €)
Assets		
Intangible fixed assets		
Software	339,857	50,454
Intangible fixed assets under development	51,661	193,138
	<u>391,518</u>	<u>243,592</u>
Tangible fixed assets		
Land and buildings	4,738,417	4,789,525
Machinery and equipment	916,945	918,446
Other fixed business assets	414,362	535,906
Tangible fixed assets under development	2,643	-
	<u>6,072,367</u>	<u>6,243,877</u>
Financial fixed assets	2,322,129	5,525,371
Current assets		
Receivables		
Trade receivables	728,538	906,709
Tax and social security contributions	-	66,864
Other receivables and accrued and deferred assets	1,982,920	1,585,488
	<u>2,711,458</u>	<u>2,559,061</u>
Liquid assets	<u>30,756,914</u>	<u>27,719,876</u>
	<u>42,254,386</u>	<u>42,291,777</u>



Liabilities

Group equity

Short-term liabilities

Accounts payable

Tax and social security contributions

Other liabilities and accrued and deferred liabilities

31 December 2021 (in €)

26,558,151

788,153

1,665,438

13,242,644

15,696,235

42,254,386

31 December 2020 (in €)

27,867,528

977,009

687,959

12,759,281

14,424,249

42,219,777



Consolidated profit and loss account for 2021

56

	2021 (in €)	2020 (in €)
Net turnover	20,754,098	20,005,965
Purchase value of turnover	-144,148	-100,810
Net turnover	20,609,950	19,905,155
Costs		
Wages and salaries	8,289,246	7,542,639
Social security contributions	787,702	847,190
Pension contributions	1,330,958	1,236,937
Other personnel costs	530,797	634,562
Depreciation	833,653	1,017,491
Other operating expenses	8,827,082	11,640,017
	20,599,438	22,908,872
Operating result	10,512	-3,003,717
Financial income and expenditure	-117,973	27,903
Result before taxation	-107,461	-2,975,814
Taxes	-1,201,916	-363,953
	-1,309,377	-3,339,408
Result from participating interests	-	6,926,231
Result after taxation	-1,309,377	3,586,823



Consolidated cash flow statement for 2021

	2021 (in €)	2020 (in €)
Cash flow from operating activities		
Operating result	10,512	-3,003,717
<i>Adjustments for:</i>		
Depreciation	820,596	1,016,799
Movement in provisions	-	-
	<u>820,596</u>	<u>1,016,799</u>
<i>Movement in working capital:</i>		
Movement in receivables	-152,396	-2,974,456
Movement in short-term liabilities	70,070	3,159,422
	<u>-82,326</u>	<u>184,967</u>
57 Cash flow from operating activities	<u>748,781</u>	<u>-1,801,951</u>
Interest received	-118,825	-55,694
Result from participating interests	-	6,926,231
	<u>-118,825</u>	<u>6,870,537</u>
Cash flow from operating activities	<u>629,957</u>	<u>5,068,586</u>
Cash flow from investment activities		
Investments in intangible fixed assets	-235,136	-
Divestments of intangible fixed assets	4,091	5,681,201
Divestments of intangible fixed assets	-579,689	-757,282
Divestments of tangible fixed assets	13,722	692
Movement in other financial fixed assets	2,644	-
Long-term lending	3,068,429	-
Income from securities	133,000	149,678
Cash flow from investment activities	<u>2,407,081</u>	<u>5,074,288</u>
Increase / (decrease) in funds	<u>3,037,038</u>	<u>10,142,874</u>
Analysis of funds		
Funds as at 1 January	27,719,876	17,577,002
Movement in liquid funds	<u>3,037,038</u>	<u>10,142,874</u>
Funds as at 31 December	<u>30,756,914</u>	<u>27,719,876</u>



07

Directors and officers



Directors and officers as of 31 December 2021

Chief Executive Officer

Roelof Meijer

Supervisory Board

Paul Schnabel, *Chair*

Mark Frequin

Simon Hania

Lokke Moerel

Kees Neggers

Jeannine Peek

59 Gerben van Leeuwen (since April 2021)

Dennis Raithel (since November 2021)

Executive Board

Cristian Hesselman, *Director of SIDN Labs*

Arjan Middelkoop, *Commercial Director*

Tuyen Nguyen, *Chief Financial Officer*

Cees Toet, *Operational Director*

Staff Council

Jeroen Roosen, *Chair*

Chris Faber

Jack van Kolck

Martin Sluijter, *Secretary*

Thymen Wabeke

Romana van der Heusen

Ruben Wubbels, *Vice-Chair*

Complaints and Appeals Board

Hendrik Struik, *Chair*

Peter Blok

Huib Gardeniers, *Secretary*

Sylvia Huydecoper

Thomas de Weerd

Dennis Wijnberg



08

Glossary



Abuse

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

Abuse204.nl

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

Access provider

A service provider that enables customers to access the internet.

Agile working

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

Anycast

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

Artificial intelligence (AI)

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

ccTLD

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

CENTR

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

Complaints and Appeals Board (C&AB)

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

DANE

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

DDoS

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

DEX

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

Dispute Resolution System for .nl Domain Names

Anyone who registers a .nl domain name is responsible for making sure that the registration doesn't infringe anyone else's rights. That can happen if, for example, the domain name makes use of someone else's brand name, trading name,

personal name or organisation name. If a registration appears to infringe someone's rights, a dispute can arise. SIDN's Dispute Resolution System has been set up as a quick and affordable alternative to using the law courts to settle a dispute.

DKIM

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

DMARC

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

DNS

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

DNSSEC

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

Domain name

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

Domain Name Surveillance Service (DBS)

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



Domain Registration System (DRS)

The system that we make available to .nl registrars for registering .nl domain names and managing existing registrations.

Downtime

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

ECP

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

eID

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

ENTRADA

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

62

FaDe

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

Fake webshop

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

gTLD

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

Hosting service provider

A hosting service provider is a business that provides web hosting services, involving the provision of storage space, processing capacity and network traffic handling capacity on a web server. As well as providing website and e-mail hosting

on a dedicated or shared server, nearly all hosting service providers also provide domain name registration services.

ICANN

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

IETF

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

(Internet) extension

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

Internet governance

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

Internet Governance Forum

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

Internet of Things (IoT)

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

Internet Protocol (IP) address

A unique combination of numbers and/or letters. Every computer or server on the internet has an IP address, at which

it can be contacted. If you visit [www.whatismyip.com](#) you can check the IP address of the device you are currently using.

Internet service provider (ISP)

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

IPv6

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

IRMA

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

Malware

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

Name server

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

NL IGF

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



Notice-and-Take-Down Procedure

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

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

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

NTP

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

NTS

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

Open source

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

Phishing

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

Registrant

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

Registrar

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

Registrar Scorecard

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

Registrars' Association (RA)

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

Registry

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

Registry service provider

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

Resolver

When you enter a web address (URL) into your browser's address bar, it is translated into the IP address of the relevant domain. The translation process is known as resolving, and the machine or software that does it as a resolver.

Resolving

Responding to DNS queries.

RIPE NCC

The Réseaux IP Européens Network Coordination Centre is the Regional Internet Registry (RIR) with responsibility for issuing IP addresses in Europe and the Middle East. RIPE NCC is one of the

world's five RIRs, the other four being APNIC (for Asia and Australia), AfriNIC (for Africa), LACNIC (Latin America) and ARIN (for North America). See also ripe.net.

Server

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

Signing

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

Spam

Unsolicited e-mail.

SPF

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

SPIN

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

StartTLS

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

Testbed

A set-up for testing a technical infrastructure.

TLD

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

Top-level domain

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

Typosquatting

A form of internet abuse that takes advantage of the fact that people



sometimes make slips when typing web and e-mail addresses. A user who mistypes an address lands on the typosquatter's site. Typosquatting is often associated with malicious activities such as phishing.

Validation

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

Whitelisting

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

WIPO

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

64

Whois

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

Zone file

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



Colophon

Publisher

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

65

www.sidn.nl
www.sidnlabs.nl
www.sidnfonds.nl

Concept and design

[Lumen Designers Network, Breda](#)

Text

Cre-Aid, Arnhem
www.cre-aid.nl

Translations

G & J Barker Translations
www.gandjbarker.co.uk

© 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

<https://www.sidn.nl/en/newsletter>