de NATRIS Consult
Connecting Visions
Creating Awareness

in cooperation with
Porte Consultancy

Setting the Standard

for a more Secure and Trustworthy Internet

The identification of pressure points in society to speed up internet standards deployment

Setting the Standard

For

a more Secure and Trustworthy Internet

The Identification of Pressure Points in Society

to Speed up Internet Standards Deployment

Author: Wout de Natris, De Natris Consult

In cooperation with: Marten Porte, Porte Consultancy

Preface

In January 2019, the Multistakeholder Advisory Group (MAG) of the global Internet Governance Forum (IGF) decided to allow for a pilot project with a clear goal: can the IGF assist in finding recommendations and potential solutions for a long-running, complex internet governance issue? The topic of choice: the implementation or deployment of internet standards. Standards that after deployment make the internet more secure and safer for all users around the globe. Standards that exist for years, even decades, but are not massively deployed. What are the reasons for non-deployment? What are the solutions, ways forward and which stakeholders have to play a role in making deployment a reality? Questions that this report sought and found answers for.

If anything, the subject proved to be urgent. In all phases of the project we could draw on contributions, assistance and input from relevant stakeholders, for which we are very grateful. From these contributions we present six recommendations, tested and debated during breakout sessions in the IGF workshop. This allowed for the identification of pressure points in society where the discussion of internet standards can bring deployment closer to reality. All these (tangible) outcomes can be found in this report.

This report can and does not claim to be complete. It is a work in progress that may have missed currently undertaken initiatives. It actively shares with you the combination of the input of participants and the research results found in the, limited, available time. It is important to understand that the recommendations and proposed next steps are the outcomes of the collective input of all participants. They do not agree on each specific step, but there are many ways to reach a satisfactory level of internet standards deployment. On one thing they all agree: deployment is a requirement for a safer and more secure, resilient internet; and that it is time to act. First, if hesitant, steps towards deployment have been identified.

This pilot project would not have been possible without the support of many individuals and organisations as shown in the first annex to this report. The following persons deserve a special mention. Without the enthusiasm of Lousewies van de Laan and Arda Gerkens at the inception of this project we might not have come this far. Without the continuous support of several organisations from the Dutch technical community and their believe in a more result driven IGF, the idea of a pilot project would never have materialised. Olaf Kolkman talked us through the technical side of internet standards. Arnold van Rhijn was a critical reader. The cover page was designed for us by Anastasiia Fito. Thank you all.

The following organisations made the work itself possible through their generous contribution. The German Federal Ministry of Economic Affairs and Energy made it possible to actively reach out to parliamentarians and present at national, European and global level on the IGF in combination with this project, leading to many parliamentarians joining the workshop in Berlin. Without the excellent cooperation with the people at Medienstadt Leipzig e.V., Sandra Hoferichter and Carsten Schiefner, and “team Jimmy Schulz” the reach out to parliamentarians would never have been such a success. The Dutch Ministry of Economic Affairs and Climate and SURFnet allowed us to do the research and write the report. DINL contributed to reaching out to parliamentarians in The Netherlands. Dutch registry SIDN and ECP (Dutch Platform for the Information Society) made the Berlin IGF workshop possible, SIDN the presentation of the results in Geneva to the MAG. ECP also contributes to the dissemination of the report.

The next phase is to make this report as widely known and influential as possible. It has already been presented at the first MAG meeting in Geneva in January 2020 and at the European Commission’s High Level Group on Internet Governance on 28 January 2020. Further presentations are foreseen, e.g. at the Annual The Hague Meeting of the Global Forum on Cyber Expertise in April 2020 and at the Dutch Standardisation Forum in May 2020. The recommendation concerning ICT education is part of the EuroDIG 2020 program. Many organisations have agreed to assist in the dissemination to ensure a global reach.

We thank all who have contributed, assisted, supported and worked with us. Without you we would never have come this far and frankly, much further than we ever expected at the start. It goes without saying that any inaccuracies in the text are ours. This report however should not be the end, but a start. We expect to be in touch soon.

Wout de Natris

Marten Porte

Haarlem, March 3rd, 2020

Table of contents

Executive summary

'*All things internet is code. It is time we all start realising this and act upon it'*[1].

To make the internet more secure is a Herculean task, as it involves multiple stakeholders with, at least at first sight, totally different and conflicting interests. At the same time every individual and organisation active on the internet has a common interest: nobody wants to be hacked, lose valuable data or have compromised systems. This is a starting point for all future debate and actions.

The internet functions on agreed upon protocols, so-called internet standards, allowing communication to take place. The original internet protocols were not always developed with security in mind. Hence the internet is inherently unsafe and prone to abuse. Add insecure websites and software, insufficient protection of data and Internet of Things (IoT) devices that enter the market without (sufficient) security built in to protect the device itself and the data and / or privacy of the customers and it becomes clear that a general situation of insecurity is the norm.

Over the past 20 years many new (internet) standards have been created and published, fixing security issues in the older ones. It is a fact that these fixes, e.g. DNSSEC, OWASP top 10, safe software principles[2], have not been deployed at such a massive scale that the internet has become a safer place. This report focuses on the reasons for the slow deployment and provides recommendations and potential future actions to change the course of internet security. Mass deployment of these standards is not the cure for all internet ills, but will cut off many options for abuse and criminality now open to criminals and others with nefarious motives. Deployment must become the standard in the world, in order to ensure a more secure and safe internet.

Reasons for non-deployment

Several causes for slow adoption have been identified. Many participants in this project gave the absence of a business case as the main reason for non-deployment. If nobody asks for the deployment of standards, let alone is willing to pay for more security, there's no demand, resulting in no supply[3]. This does not explain all. This report shows that the lack of any pressure from any angle, makes the voluntary internet standards easy to ignore. This report shows that there is more than just the lack of a business case, it is a lack of almost everything.

[1] Slightly adapted interview quote

[2] In annex 3 an explanation can be found explaining the six examples this project has used to extract relevant information from the community. Three are internet standards, DNSSEC, RPKI, bcp38. Three are not: the OWASP top 10; ISO 27001 and; Safe Software Principles. To provide for an ease of writing and reading, we have stretched the meaning of internet standard for this report, fully acknowledging the official definition.

[3] For an extensive study read 'Economic aspects of Internet security', Henk Kox and Bas Straathof, CPB

Lack of mandatory standards

Internet standards are not standards according to laws. In a legal sense they hardly even exist[4]. When relevant EU Directives and other government documents mention officially recognized standards, it usually is to point to: 1) consumer rights / actions; 2) the necessity to avoid administrative costs; 3) to avoid legislation in general; 4) voluntary deployment. However, in recent years a shift in thought and opinion can be noted.

The status quo is in contradiction with a widely adopted norm: the protection of the public core of the internet. This norm is seen as important in order to protect the internet that is free, open, interoperable, secure, and resilient. One aspect of this core that needs protecting are the standards that make the public core of the internet function. As far as this report has been able to establish, these internet standards are currently only to a very small extent covered by law or legally binding regulations. That makes them unprotected, as is the public core as a whole[5].

There is a second relevant contradiction. The (internet) industry and manufacturers of devices have to deploy internet standards. However, with the exception of more interest in securing IoT devices, it is the consumer that receives full policy attention from governments (and private sector, e.g. banks) in many publications and actions relating to cyber security. Just about the only stakeholder group that has hardly any influence over most aspects of this issue[6].

Lack of cooperation

Internet standards are made within the so-called technical community[7]. Because this work is highly technical, the work and the outcomes are fairly isolated. The technical community tends to advocate its results primarily within its own group. Unfortunately the efforts of the past 20 years have not led to mass deployment. At the same time the work of the technical community impacts (government) policy and has technical, financial and educational implications for those having to deploy. This calls for new relationships and changes of narrative. To make internet standards deployment normal, it is of importance to make them better known, in a language all can understand and stresses the need for deployment to the board room. This report calls for bringing the different stakeholders, e.g. policy makers, technical community, trade and consumer organisations, regulators, educators, parliamentarians, human rights experts and child protection activists, leadership and media, together to work on trust, cooperation, narration and dissemination with one goal in mind: deployment.

The creation of standards is a highly technical collaboration. As such the technique must not be over-estimated. The decision to deploy the resulting standards most likely is made by non-technicians. This is an important insight, leading to a desirable change of approach, narrative and cooperation.

[4] Only one example this project uses, ISO 27001, is an “official” standard

[5] The fact that the NIS Directive mentions the public core in lemma 14 may be a first step in a new direction

[6] Awareness programs and training are extremely important, but a change of focus is called for if a more secure and safer internet is the goal

[7] This community also includes internet resource organisations responsible for the distribution of internet resources as e.g. domain names and IP addresses, and Internet exchanges. As they do not create internet standards, this report categorises them separately.

Lack of e-skills in curriculum

Apart from the fact that contributors to this report have opined that some standards, e.g. DNSSEC, may not have been thought through sufficiently from a practical, deployment point of view, it is also necessary to point out that the people having to deploy may not all have sufficient skills to do so. Education curricula, e.g. from the vocational level in building secure websites, to writing and testing code during its creation at university level, in general put insufficient emphasis on internet security and internet architecture. This has to change and become part of schooling at all levels.

Collective action problem

Summing everything up, it comes down to a collective action problem. No one wants to move first in a situation where there is essentially nothing stimulating deployment, with the exception of some initiatives that certainly work in the case of those willing to change for the better; voluntarily. They are presented below.

The following is a worrying conclusion, but true. In the current situation by not deploying these standards, the (internet) industry more or less facilitates abuse and crime. Not in a conscious way, but the current inaction, puts everyone in permanent danger.

Time for action!

"*Once the relevant standardisation activities, specific standards or technical specifications needed to support a policy or legislation have been identified, it is important that they are widely disseminated, used and implemented. It is also important that the respective policy contexts, in which specific standards are to be used, are highlighted with broad stakeholder involvement, and that awareness is raised on the importance, benefit and need of using the standards within the policy contexts*"[8].

If the goal of this report was only to identify the problem, underscoring recently formulated norms could have sufficed. However, the time has come for this debate to move beyond the identification of relevant ICT standards and norms. To move beyond the "if only they / it would-could-should" phase. It is time to advocate action. Many relevant stakeholders know about the deployment option in front of them. This report identifies stakeholder groups that have to collaborate, exchange information and knowledge, who have to build trust, but also acknowledge what topics they need to work on together and agree upon. What will be a defining point in working towards success, is not only the question on who needs to feel responsibility, but primarily who is willing to take ownership of what critical issue concerning deployment. And, the will to step out of comfort zones. This will decide on chances to succeed. Having recognised this, let's proceed, by looking at the identified pressure points in societies.

[8] ROLLING PLAN FOR ICT STANDARDISATION 2019, European Commission https://ec.europa.eu/growth/content/2019-rolling-plan-ict-standardisation-released_en

Pressure points

Working on the issue, it became clear very soon that the issue of the deployment of internet standards has multiple angles that need addressing before a change of course can take place. There are so many and different stakeholders involved, who can all make a difference in their respective way. All these angles make it easy to lose focus and a clear sight on the road ahead. This report presents so-called pressure points in society, where interest in the topic can be expressed, actions demanded or discussions started, putting pressure on the organisations that need to deploy. The pressure points show what role respective stakeholders have to play. Reaching out actively to these (absent) stakeholders and get them involved, is an important task for 2020.

Recommendations

Based on the input from all the participants six recommendations are presented, from which potential actions were developed that are presented in this report. These are the recommendations.

1. '*Create a business case for the deployment of internet standards*'.
2. '*To deploy internet standards successfully they need to be incorporated by reference into law or legally binding regulations, including a designated regulator*.'
3. '*To deploy internet standards successfully requires building security by design / default into products and services*'.
4. '*All stakeholders should collaborate on coherent strategies for multilingual awareness raising on internet standards and their effect on internet security'.*
5. '*Internet standards and architecture must become part of education curricula*.'
6. '*Standardisation processes are advised to include a consultation phase with government and industry policy makers, and civil society experts*.'

Suggestions for follow-up

Stemming from the recommendations and the pressure points, several actions are suggested in the form of working and study groups, including relevant stakeholders of which some are currently not actively involved (in the IGF).

To change the status quo is a Herculean task that needs collective action. In such cases most people tend to look at the government for guidance. Concerning the topic of internet deployment, a paradox came to light: Not a single participant indicated to want legislation, yet when asked for the solution to deploy there is a rough consensus among the same participants that governments need to have, at a minimum, a guiding role.

Perhaps it is time this topic is looked at from a different angle. If internet security is seen as a health issue, albeit digital health, what options are available to the world to deploy internet standards? Who needs inoculating first? Let’s first take a step back and present on how we got this far.

Part 1. Background

Fairly shortly before the Internet Governance Forum (IGF) in Berlin Vint Cerf, one of the 'fathers of the internet', gave an interview. He advocated the deployment of several internet security standards, including some discussed here: "We need to be less naive if we're going to fix it"[9]. In the following this report present recommendations and potential ways forward to get there.

1. Introduction

So, why are internet standards adopted so slowly?

In January 2019 the Multistakeholder Advisory Group (MAG) of the Internet Governance Forum (IGF) agreed to a pilot project in the form of intersessional work on the topic 'implementation[10] of internet standards'. The suggestion for a pilot followed on an advice given to the MAG via the MAG Working Group Multi-Year Strategic Work Programme (WG-MWP). The WG-MWP had the following goal:

> *"The MAG WG … was chartered by the MAG to see what "... more could be done to take a strategic, long-term view of the role and activities of the IGF...to reinvigorate the IGF by taking a longer-term view of particular issues ... achieving concrete outcomes on these over time. A longer time horizon ...could help to bring in new collaborators, including international agencies, and new donors.[11]"*

This intention matched with the long held and explicitly expressed view of several representatives of the technical community in The Netherlands. These organisations actively supported the second iteration of the report 'Strengthening Cooperation Within the Context of the IGF'[12], developed within the WG-MWP. In the report practical options and solutions are provided, formulated by the IGF community at large[13]. One recommendation being a pilot aimed at finding solutions and potential ways forward for a long-lasting and complex internet governance issue that is in need of one. After deliberations with potential supporters of this pilot, the topic of choice became the deployment of internet security standards that, once deployed, would make the internet safer for all users, immediately. The MAG agreed to the, self-funded, pilot. The assistance of the IGF secretariat and a workshop slot at the IGF were guaranteed.

[9] Interview on Quartz, 6 September 2019, https://qz.com/1703322/internet-pioneer-vint-cerf-on-what-we-need-to-do-to-fix-the-web/ (accessed 7-11-2019)

[10] The words implementation, deployment and adoption are used in texts for the same principle. The technical community who created the standards favours deployment. We will use this term from here on.

[11] 2018 WG on IGF Multi-year Strategic Work Programme. https://www.intgovforum.org/multilingual/system/files/filedepot/67/wg_on_igf_2018_multi-year_strategic_work_programme.pdf.

[12] https://www.intgovforum.org/multilingual/filedepot_download/5075/1442.

[13] At the 2017 Geneva IGF a day 0 workshop was organised around this topic. See the intention and report here: https://igf2017.sched.com/event/CRB6/strengthening-cooperation-within-the-context-of-the-igf-creating-a-roadmap-for-2018. It is an example of how a workshop can be used to gather information aimed at tangible outcomes of the IGF, i.e. the report under footnote 8.

1.1. Project goals

The main goal of this project is to find ways forward to speed up the deployment of internet standards, such as DNSSEC, RPKI, OWASP top 10[14]. Of course, the goal had to be specified to make it workable in the limited time available for this research. The work focused on four goals: determine the causes of slow deployment; bring different, and new, stakeholders to the discussion; formulate practical recommendations; actively disseminate the outcomes. This is found in part 2 of this report.

In a way this pilot project tested the capability of the IGF to address a complex internet governance issue and deliver tangible outcomes. Can such a project generate traction? Will people commit, share relevant data, etc.? This “test” is not the main focus of this report. We address it in part 3, chapter 9.

1.2. Methodology

The main part of the outcomes in this report are distilled from the contributions received from within and beyond the IGF community. A survey was spread, at national, regional and global level, through the IGF, industry and technical organisations. The information thus gathered resulted in a set of concept recommendations. They were debated and tested in five break-out sessions at the IGF and through interviews with representatives of many (internet) organisations. The combination with desk research connected several dots and led to the identification of pressure points in society that can contribute to deployment. Chapters 2 to 6 provide more in-depth information.

1.3. Urgency

There is a clear reason why these internet standards exist: they patch flaws in the original internet protocols. Protocols that were not designed with security in mind. The existing flaws allow abuse and attacks. The newer standards presented here, repair these flaws, give guidance on how to design more secure products and services and to secure information. Every day the world stalls in taking action towards deployment, more (serious) harm is afflicted on ever more users, as the daily stream of incidents and successful attacks show.

1.4. Results

In chapters 7 and 8 the outcomes, conclusions and ways forward are presented. No one who participated disagreed that some form of action is necessary. The differences lie in the how. Hence the recommendations are the accumulated outcome of this process, without choosing between them. There is not just one route towards deployment. Most likely a combination of efforts is the right way forward.

In short, this report contributes to answer a complex question that is becoming more relevant by the day: How can the internet become a safer, more secure place for all its users?

[14] These standards are explained in annex 3 this report.

Part 2. Report on internet standards deployment

2. Origins of standards

This report highlights a specific subset of six (internet) standards and protocols. Three are internet standards, three are not. They are examples, so the list is incomplete where relevant standards and standards organisations are concerned. Hence this report refrains from giving one all-compassing definition of an internet standard in the context of this report. All six examples, through mass deployment, make certain parts of and devices connecting to the internet safer, indiscriminately, immediately. As a warning, only in this context should they, collectively, be read as internet standards, for the purpose of ease of reading and writing this report.

2.1. What is an internet standard?

"*In computer network engineering, an Internet Standard is a normative specification of a technology or methodology applicable to the Internet*"[15] or in the words of the Internet Engineering Task Force (IETF): "*In general, an Internet Standard is a specification that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet*"[16]. Wikipedia adds that internet standards are made exclusively by IETF.

Internet standards in the classic sense are IETF-related. Yet there are other standards related to the internet and internet connections[17].

The Open Web Application Security Project (OWASP) produces protocols of relevance to secure websites and where safe software is concerned there are several initiatives that strive for more secure coding before a product is launched. Several standardisation bodies produce voluntary and mandatory standards, like e.g. ISO, NEN, NIST, ETSI, etc.[18]. One standard that is used as an example for this report, ISO 27001, falls under this category. There are some industry initiatives introducing self-regulatory proposals, e.g. the Safe Software Alliance's principles are introduced here as a "standard". It is important to stress the following word: voluntary. Most of these standards and protocols are voluntary to deploy. Some have to be deployed because otherwise connection to or transport to parts of the internet is impossible, yet this does not make it mandatory.

[15] https://en.wikipedia.org/wiki/Internet_Standard, accessed 2-1-2020.

[16] RFC 2026, https://tools.ietf.org/html/rfc2026.

[17] E.g. The World Wide Web Consortium (W3C), the Institute of Electrical and Electronics Engineers (IEEE)

[18] We do not elaborate on any of the organisations mentioned here nor on their inner procedures, etc., as they are not a part of the scope or the goal of this report.

It is important to understand that most of the standards that make up the internet were created in a time before its mass use started, when only the military and employees of a limited number of U.S. universities communicated with each other over the internet. As Vint Cerf explains:

> *"Four decades ago, when Bob Kahn and I were creating the TCP/IP networking protocol for the internet, we did not know that we were laying the tracks for what would become the digital superhighway that powers everything in society from modern business to interpersonal relationships"*[19].

The protocols or internet standards, in other words were created without security in mind. At best it was considered, after which it was decided security would not be a priority. All the standards that are discussed here can in a way be seen as digital band aids, fixing what only in hindsight was flawed.

2.2. Internet standards within this project

In this project six different standards and protocols[20] are mentioned: DNSSEC, RPKI, bcp38, OWASP top 10, ISO 27001 and the principles of the Safe Software Alliance[21]. In the context of this report they are used as examples, as there are many more standards that need to be deployed to make the internet a safer place. The six were not randomly chosen though, as each one in its own way would make the internet instantly a safer place, were it to be deployed massively. The examples found their way into this project after consulting with representatives of the technical community in The Netherlands. They were chosen in such a way that they see to a wide range of products and services on and surrounding the internet, including very different organisations in development as well as in deployment.

It is also of importance to understand the following, as will be explained more in-depth below: Internet standards are not standards in the context of law, with the exception of ISO 27001.

Secondly, OWASP top 10, ISO 27001 and the principles of the Safe Software Alliance are not internet standards in the usual sense, as described in the paragraph above. As this report focuses on securing the internet and the devices connected to it, the term 'internet standards' is used in a wider sense.

[19] Quartz https://qz.com/1703322/internet-pioneer-vint-cerf-on-what-we-need-to-do-to-fix-the-web/ (accessed 7-11-2019)

[20] See Annex 3

[21] From here on we will use the word "standard(s)" to encompass all six examples used for this report, except when specifically mentioned separately.

3. Overview of the problem

> *"Given how critical DNS is to the functioning of the Internet, it's a mystery that the world is prepared to accept such a security-deficient protocol at the core of all its infrastructure. What's even crazier is that there's a secure solution that's been in the pipeline for over a decade: (…) DNSSEC"[22].*

Since the early days of the internet, it has, without exception, always functioned. People might think therefore that no problems exist, and why fix something if it isn't broken? This could not be further away from the truth. Even though the internet, in general, works; as our dependency grows, the fundaments of the internet become shakier every day.

3.1. Importance and urgency

For many, the importance of the implementation of the mentioned internet standards will not ring a bell. On the other hand, nobody will be able to argue that cyber security is of no importance to our society. Following are two examples of documents giving importance to this threat.

NIS Directive

> *"The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union"[23].*

European Cyber Security Perspectives 2019

> *"2018 is a difficult year to summarize for Infosec. After the initial flurry of activity around Spectre and Meltdown in the beginning of January, we ended the year with global supply chain concerns brought about by the Super Micro story. Throughout the year we saw the geopolitical dilemmas of 2018 manifest in cyber security issues. Technology giants like Facebook and Google had a security reckoning. However in pure scariness the medical data breaches of MyHeritage (DNA) and MyFitnessPal (health) rank higher. The Starwood Marriot Hotel breach made every travelling executive nervous for the rest of the year, but probably not as nervous as the incident of CEO Fraud at Pathé"[24].*

Two examples from the many that could have been quoted. One from the public sector and one from a public-private partnership. These examples show that cyber threats are increasingly on the radar of

[22] 'Why isn't everyone using DNSSEC?' Nicolai Hampton, 2017 https://blog.apnic.net/2017/06/28/isnt-everyone-using-dnssec/ (accessed 18-12-2019)

[23] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, page 1

[24] European Cyber Security Perspectives 2019, Volume 6 https://www.thehaguesecuritydelta.com/media/com_hsd/report/225/document/ecsp-2019-european.pdf

officials and businesses. What is however rarely mentioned, is how many, if not all, of these attacks originate from flaws in current internet standards and protocols. Flaws that the deployment of said standards could, at worst, mitigate and, at best, mend. The urgency of cyber threats is felt, which is shown by the words of the authors. Yet, the world stalls in taking some form of action towards deployment of improved internet standards. Every day, more (serious) harm is afflicted on ever more users, as the daily stream of incidents and successful attacks show.

Is deployment of standards on the internet really so slow? Researchers from The International Association for Cryptologic Research (IACR), have said the following on the deployment of RPKI: "*Despite extensive effort, RPKI's deployment is frustratingly sluggish, leaving the Internet largely insecure*" [25]. In a research paper for USENIX, the advanced computing systems association, the deployment of DNSSEC is characterized similarly: "*Despite the effort being poured into DNSSEC, actual deployment of signed records at the end- system level has remained quite limited* "[26]. These are just two examples of internet standards that would greatly increase security, but where deployment is not making the necessary progress. It is known that the problem exists and has serious consequences, but why not just wait till the market solves this problem at its own pace?

3.2. 5G and Internet of Things

5G mobile networks are generally believed to give connectivity a tremendous boost. It will provide the bandwidth and the speed for even more devices to be connected to the internet. It might start the age in which Internet of Things (IoT) will truly take off. This would mean millions, or billions of devices being connected to the internet in the coming decade. To ensure safety in the number of devices currently at hand is already a tremendous challenge. As it will e.g. include the security of your home appliances and autonomous functioning systems, the fallout of security flaws will be even more tremendous. These prospects set in fact a deadline to step up our cyber security game. If the internet community does not get threats under control before every part of our everyday life is connected to the internet, the problems will be countless. This makes the need of adopting security standards an urgent task. "After 5G deployment we are lost forever"[27], as someone we interviewed said.

Now that the threats and the urgency to find a solution has been analysed, why have solutions not been successful enough to date?

3.3. Collective action problem

Imagine a sidewalk after a snowy day. Everybody would benefit from having a sidewalk free of snow. Especially the vulnerable citizens with bad mobility could be harmed if nobody would clean their

[25] *Are we There yet? On RPKI's deployment and security* https://eprint.iacr.org/2016/1010.pdf

[26] Measuring the practical impact of DNSSEC Deployment https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_lian.pdf

[27] Interviews were conducted on the basis of non-attribution. The names of those interviewed are in annex 2

sidewalk. But it is cold outside, and all house owners on the street ask themselves: why should I be the first to clean my part of the sidewalk? Nobody else is doing it. And I won't even benefit because I'll still have to cross other people's snowy sidewalk. No one feels to move first, because it costs them energy while the benefits are marginal, or non-existent. Yet, if everyone cleaned their part of the sidewalk, the neighbourhood would be protected, and everybody would benefit from the work that's been done.

To solve such a problem, citizens might be convinced to take action, since they just need to invest some energy, but what if we're talking about private companies in a highly competitive market needing to invest large amounts without clear advantages to themselves? Unfortunately, this is exactly the kind of situation the internet finds itself in now. The question now is: how to turn this around?

Just like the sidewalk, the issue of internet standard deployment is a classic case of a collective action problem. This is "*a situation in which all individuals would be better off cooperating but fail to do so because of conflicting interests between individuals that discourage joint action*"[28]. In this case, with notable exceptions, no individual organisation wants to be the first mover, as it does not profit from its move, its customers do not ask for it, the actions to be taken costs resources of several kinds and cannot, easily, lead to extra profit or higher margins. For all these reasons, collective action seems to be the only way forward while at the same time keeping a level playing field.

As is a premise for any functioning market, there needs to be a level playing field between competitors. This means as much as that every player should play by the same rules and has the same initial chances on success. As is the case in the internet industry, where currently the collective action problems in the market cannot be solved. The current situation exists in which there is no carrot nor a stick. As one of our interviewees formulated it: "no one cares if you deploy and no one cares if you don't". There is absolutely no incentive to do so. Both positive and negative incentives will play a part in this report.

Currently, the collective action problem creates somewhat of a negative business case, stimulating non-deployment.

3.4. (A negative) business case

What can be seen when looking at the costs and the benefits of deploying some of the internet standards is that the two are not aligned. The implementing player makes developing and deployment costs, that do not translate into direct benefits. This is for several reasons. One of them being that for a standard to be reciprocal in its effect, both the sending and the receiving side need to have it implemented. On top of that, the abuse and attacks usually can still reach the first mover, since those who have not deployed still send malicious traffic and content, while they might receive less abuse themselves because of the security offered by the deploying network. So, the first mover only stands to lose resources while not or hardly gaining any competitive advantage. Furthermore,

[28] Oxford University Press. 2018-01-18 via Wikipedia https://en.wikipedia.org/wiki/Collective_action_problem (accessed 20-01-2020)

customer requests to deploy will be minimal regarding the complexity of the matter, let alone that customers will be willing to pay extra for it. This in combination with people's natural assumption that it will be others, not them, who will be faced with internet abuse and the corresponding financial damage, makes for huge challenges in the deployment of internet standards in a market-driven way. Later this report will have a look at the possible solutions from this angle of the problem. For now, let's dive a bit deeper in some of the problems on the business-side of things.

3.4.1. The internet industry

One of the reasons that market-driven forces have not driven up the deployment of standards could be the specific nature of the internet industry. In many markets, margins on internet infrastructure services such as Internet Service and hosting Providers are so slim that they do not allow for players who would be intrinsically motivated to implement the security measures. This is because they might simply not have the financial buffers to take such risks. Also, internet users have become acquainted to use services on the internet for free. Gmail, Hotmail, WordPress, blogs, Flickr, WhatsApp, etc., etc., are all internet services provided for free. There are numerous costs involved for the service provider, but these are not being charged to the user. It has become normal for users to think the use of internet is free and as a result do not (think about having to) pay for a secure service. Being a "user" instead of a "customer" also results in not having much leverage in a discussion about the level of security offered. Finally, and this is another important factor, the digital environment is badly understood by users. People have a sense of brakes in relation to a car but will completely freeze when they even hear someone utter the word 'IP-address'. Secure or insecure, the internet is something intangible for the most users. They take it for granted without understanding how it works.

3.4.2. Wrong expectations

One of the consequences that the internet for many users is something hard to understand, is that many use platforms which will host our mail and websites in our stead. Many users will therefore refer to their website builder or platform when asked about their website security, assuming that they will have the appropriate skills and have set in motion actions to ensure safety. They are usually unaware of the fact that for a platform or website builder to do more for security than the bare minimum, if even that, a specific request from the customer is necessary. People will automatically assume that if not the platform, the government will have set certain standards that everyone will adhere to.

So, it appears that users of the internet badly understand the environment they are active in. This in its turn leads to unawareness in issues concerning security. People are not used to ask questions about, let alone pay for these issues. This at least in part contributes to the negative business case for internet standards deployment by the internet industry. Part of this report will focus on how to change this frame of mind. Further on the report focuses on the player who usually comes into action when collective action problems have been determined: the government.

3.4.2.1. Some examples

To give some examples of institutions that citizens generally trust to ensure our online safety. The earlier quoted blogpost by Nicolai Hampton also puts focus on financial institutions: "*Unfortunately, the uptake of DNSSEC is less than stellar. In a quick scan of my local Australian financial institutions, I found zero uptake of DNSSEC*"[29].

The banking industry is a very obvious target for criminals as there is a lot of money to be had. Phishing is the technique that almost everybody is familiar with. People receive an email stating it is necessary to change their password by clicking on the provided link, which leads them to a fake environment resembling their bank's. The criminal steals the current password this way, logs in and empties the bank account[30]. So, making sure a bank's domain name is signed and verified, DNSSEC, would seem like a priority. Financial institutions have cyber security high on their priority lists, but somehow DNSSEC is not, for reasons currently unknown in the context of this report. In annex 8, the results of pulling the domain name of the biggest banks of the biggest economies from different continents through internet.nl to check for DNSSEC deployment in 2020 are showcased[31]. The results are as abysmal as they could be, for one of the most crucial institutions that people depend on to trust[32]. The phishing scorecard for Dutch banks shows a slightly more varied sight, though not one to become overly optimistic about[33].

Apart from banks, also the companies that assign domain names to people seem to be scarcely protected: "*A look at the ICANN report on domain name registrars that support DNSSEC for .com.au and .net.au is similarly depressing*"[34], continues Hampton. There appears to be a world to win.

And lastly, the player that you might expect the most from: the government. The test results for EU eGovernment websites show that less than 50% of these websites have a positive score and failed to make 8 to 10 of 14 tested security measures[35].

3.5. Internet standards and the law

When one thinks of collective action problems, usually the government comes into play, introducing laws and regulations to make sure that everybody plays their part. But before presenting on what would be desirable or helpful in this regard, first there is a need to know the current state of play regarding internet standards in laws.

[29] 'Why isn't everyone using DNSSEC?' Nicolai Hampton https://blog.apnic.net/2017/06/28/isnt-everyone-using-dnssec/
[30] For more information: https://apwg.org/
[31] https://internet.nl/
[32] Scorecards are from Internet.nl
[33] https://www.phishingscorecard.com/ScoreCard/Netherlands/Banks/MS0x (accessed 03-02-2020)
[34] See note 30
[35] Internet.nl en de EU eGovernment benchmark. Roel Geilleit, CapGemini 2019 https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2019/10/eGovernment-Benchmark-Insight-Report.pdf

In the following, the focus will be on what has been found in formal texts and documents[36]. In the EU cyber security context standards are brought forward in a broad and rather vague way. "*Given the global nature of security problems affecting network and information systems, there is a need for closer international cooperation to improve security standards …*"[37]. "*Operators of essential services and digital service providers should ensure the security of the network and information systems which they use*"[38]. Internet standards as discussed here are not mentioned in the Directive, in fact they are excluded. Only "international standards" or "accepted standards" are mentioned, as the description of the term standard under point (1) of Article 2 of Regulation (EU) No 1025/2012[39] excludes all the standards central in this report, with the exception of the ISO 27001 standard[40]. Also, in the European Electronic Communication Code[41] standards are mentioned, but not further defined. In lemma 93 the Commission states: "*Standardisation should remain primarily a market-driven process*", handing primary action over to industry, before summing up potential exceptions that hold no link to security[42].

Is this different for the U.S. or Australia? No. The 'Core Baseline' contains security feature recommendations for IoT devices. It "*is not a set of rules for manufacturers to follow*"[43]. The Australian government released a call for views in December 2019 in search of a voluntary code for industry to follow, because "*the Government expects devices are designed with basic cyber security features so that Australian consumers can work and live securely online*"[44].

As can be seen, after one and a half decade of non-deployment, the internet standards that are at the very heart of the internet infrastructure seem to have no official recognition in laws or official documents. Nor does it seem like any incentives have been created in assisting organisations towards deployment. Until recently it almost seemed like the deployment of the already existing internet security related standards was a topic to be avoided in legislation and other legal texts.

Change can be noted though. In order to have secure IoT devices, EU negotiations are currently being held to formulate essential safety or security requirements and incorporate them into the EU Radio Equipment Directive as a basis for future European harmonized standards. But for now, it is still safe to state that at best internet standards play an insufficient role in political debates and decision-making. A conclusion that is underscored in the outreach to parliamentarians this project was able to do. For nearly all the topic was new. But why is this so? Is this because:

[36] This report does not pretend to be complete. Reflected on is what was found or provided.
[37] NIS Directive, page 7
[38] Idem, page 8
[39] "NIS Directive art. 4.11
[40] Art. 2.1 of REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European standardisation, states: "'standard' means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory …".
[41]DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code, page 53
[42] Idem, page 53
[43] https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices (accessed 9 December 2019)
[44] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice

- There is a lack of knowledge on internet standards?;
- There is a lack of communication between some of the key players?;
- The standards are produced by bodies not recognized by governments?;
- Policy makers and parliamentarians believe this would be an undesirable meddling in internet affairs, potentially stifling innovation?;
- Of the relative isolation in which internet engineers and bodies operate?

These are just some examples of questions that need an answer if society wants to find ways forward to get internet standards deployed faster.

The absence of mentions of internet standards in official communication is not a problem per se. It can be stated though, that deployment is lacking, and (near[45]) complete non-intervention from the state has not seen a market-driven deployment of said standards. By showing that standards are not mentioned, it can be ascertained that there is no political debate nor a strategy at the organisational level of society where most collective action problems are being dealt with: the government. The government can be one of the players in finding a solution, but there are also valid reasons to be weary of government involvement.

3.6. Mistrust of Governments

‘Who is the government?’ This is a question several participants have put to us, followed by ‘what is the interest of particular parts of the government where the security of the internet is concerned?’. This is a cause of the mistrust between the technical community and even, as shown below in this report, between the CSIRT community and (its own) government(s).

National governments work on national security from several angles. This leads to one department wanting a, secure, open and reliable internet for economic purposes, while another department advocates backdoors in programs and services, leaving the country and economy exposed to potential harm by third parties. Also, the protection of privacy or consumers and the internet as a whole does not always match the economic interests of companies, leading to sub-optimal or even bad outcomes for internet security.

These findings make a clear policy towards the deployment of internet standards complex. There is also no unequivocal answer to what policy prevails nor with whose and what’s views and interests opinions actually are exchanged.

This is a finding this report cannot pursue, as national governments always are sovereign in their respective policies. They are able to notice and perhaps learn from the recommendations in this report and take them into consideration when creating new policies.

[45] There are examples of awareness and/or incentivizing programs

3.7. Absence of Internet standards in the cyber norms debate

Of course, not all collective action problems have to be solved through government intervention. Maybe voluntary norms are just not a big enough part of the discussion. Through this research and analysing others' work, it can be established that the standards that are investigated in this report stand isolated in the world of cyber norms. This conclusion can be especially reached after studying the Norms Observatory of the Global Commission on the Stability of Cyberspace (GCSC).

The Hague Centre for Strategic Studies (HCSS)[46] carried out a comparative study as a part of the work of the Global Commission on the Stability of Cyberspace (GCSC), called the GCSC Norms Observatory, a custom tool with the purpose of mapping the cyber regime complex. It is designed to give answers and insights to the following:

> *"The GCSC Norms Observatory makes use of a combination of analytical methods, including social network analysis, text mining, and machine learning. The resulting model allows for the mapping of the cyber regime complex in the form of a social network. In this network nodes are norms, principles, CBM's, and initiatives. Each of these nodes represents a written text that contains a normative principle on cyberspace, for a total of 906. Connections between nodes ... are made based on either a shared thematic similarity or shared language between nodes. As a result, the layout of the network is a mapping of which nodes are connected and which policy making clusters exist within the larger regime complex"[47].*

This is captured in the following graphic[48]:

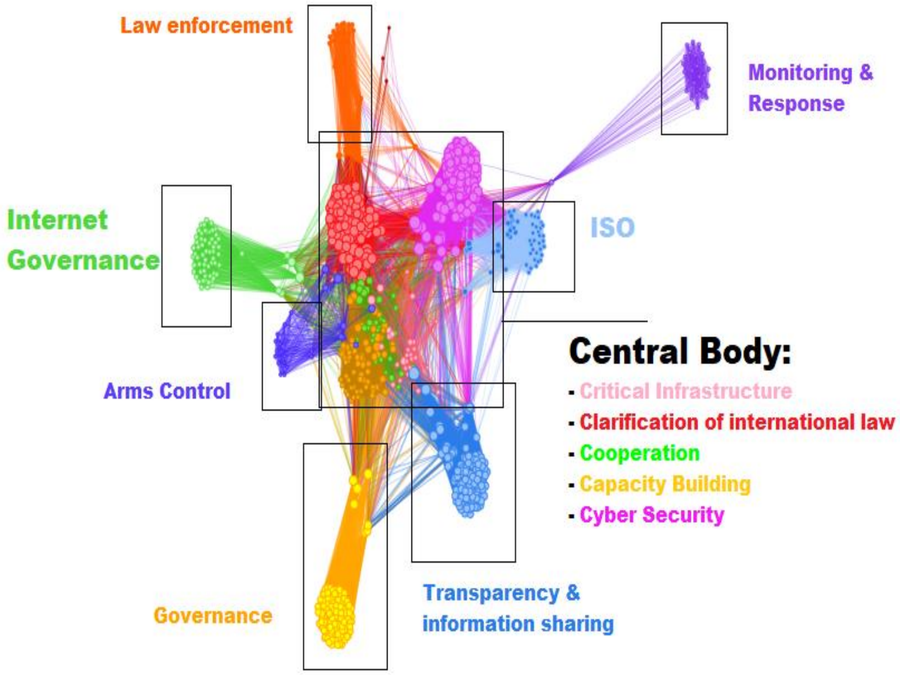


Figure 1. GSCS Norms Observatory

[46] HCSS was the secretariat for the GCSC
[47] Contribution Paul Verhagen, HCSS
[48] Graphic provided by Hague Centre of Strategic Studies

What makes the graphic on a very specific level of interest to this report, is that the technical standards securing the internet directly on implementation, in all the texts studied and analysed, some 900 in total, can only be found in the top right corner of the graphic under “Monitoring & Response”. As can be seen, the connection with all other groups is one single node. In other words, “our” standards “*only share very few thematic or linguistic similarities with the larger network. In fact, the Monitoring & Response cluster is only one node away from being completely separated from the network*”[49]. This node includes texts in formal documents where the necessity or desirability for deployment is stressed, “should, would, could”. If this node falls away, internet standards no longer have any connection to the general debate concerning internet at all, resulting in total isolation.

[49] Contribution Paul Verhagen, HCSS

4. Key Players

The governance of the internet is by nature multistakeholder and exists of many different players. For our subject in particular, several potential key players have been identified. Each for different reasons, but all have a role to play. Some currently do not have a formal role or do not take up a role. Who are they and what (potential) roles can be identified?

4.1. Technical community

The technical community in this context is the community who creates the internet standards[50]. As a few participants pointed out to us, the position and output of the technical community and internet engineers has changed over the years because the internet has become ever more important. There is a need to understand that the role the IETF has where the creation of internet standards is concerned is not neutral and has implications for other stakeholder communities, e.g. in policy, investments, security, etc.

This suggests a different approach is called for. There are two sides to this approach. If the technical community does not want governments to interfere with its processes, it is of importance that governments understand what, e.g. the IETF, does, what the relevance of what it produces is and what could go wrong if standards were to be regulated or IETF's inner processes be interfered with. Active reach out could solve this. Most likely, by far most involved outside of the IETF would welcome and embrace the information.

This form of reach out is possible, as the action of the CSIRT (Computer Security Incident Response Team) community shows, when it worked with the OECD on a report for governments on the work of CSIRT, explaining in detail what a CSIRT does and the conditions under which it can successfully cooperate[51]. Active outreach was a recommendation in the report of the IGF Best Practice Forum CSIRT of 2014. Despite the fact that at the time of writing direct contact was seen as undesirable in the CSIRT community[52], the recommendation was followed up and successfully so. This route is open for the technical community as well and one that is strongly recommended.

The second point identified is for the technical community, perhaps in association with Internet Society, to make deployment itself and communication on new standards a part of the process and thus set a first, important step towards deployment of the standards.

[50] In the IGF context it usually also comprises the internet resource organisations, internet exchanges, etc. In this context it is necessary to separate them.

[51] GUIDANCE FOR IMPROVING THE COMPARABILITY OF STATISTICS PRODUCED BY
COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs). DSTI/ICCP/REG(2013)9/FINAL 8 June 2015
https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINAL&doclanguage=en

[52] https://www.first.org/global/governance/bpf-csirt-2014-outcome.pdf

4.2. Industry / manufacturers

Industry here must be read as service providers of internet services, manufacturers of (IoT) devices and software. Organisations that have to deploy one or more of the standards.

In an ideal world internet (related) products and services would be secure by design. An ideal world where: Manufacturers of products designed to connect to the internet have security built into that product; Where after the purchase and before connection customers are obliged to provide a unique, strong password before hooking up the device; Where the software within the device however, has been hacked multiple times during the production development process; Where website builders only deliver websites that at a minimum contain the OWASP top 10; Where platforms provide an amount of cyber security that makes their customers safe at a reliable level; Etc., etc.; Where a level of security exists that it is paid for, without an option to opt out of that level of security.

Ideally industry would sense the urgency to act as they are, should be, one of the main protectors of its customers and ultimately society as a whole. Almost like the difference between a well-trained soldier and cannon fodder[53]. How to get there?

4.3. Industry / trade organisations

These organisations traditionally exist to represent their respective members and make sure the interests of the community as a whole are made known in the right places, e.g. through lobbying. Outcomes and changes in legislation that affect the membership are communicated. Members can also ask for specific trainings or newsletters. They seldom represent common or desired views towards their members as this is not what they are designed to do. Apart from the fact that all members are competitors.

Having concluded this, these organisations are one of the few places where a large part of a specific industry or trade can be reached through. As such they have to become convinced that they can play an important part into conveying the messages of standards deployment towards their members. The place where easy to understand examples and the route to deployment are created. Also training programs to deploy standards could be made and provided at this level or to provide security scorecards to members assisting procurement of secure internet services and products. This could be more effective than training individuals who may be the right persons technically, but do not have the decision power to deploy.

Trade organisations must be understood as all trade organisations of relevance to this discussion. They are potential partners in the proliferation of the knowledge and importance of internet standards, safe products and software deployment, including training.

[53] 'De toeleverancier als kanonnenvoer', (*The supply industry as cannon fodder*) Wout de Natris. Marineblad 5, jaargang 127

4.4. Platforms

The most common description of a ‘platform’ in our use case is a digital platform where customers and suppliers come together around a special service. In this context it is seen as a digital place where many, usually private persons and SMEs use a (free) online service as e.g. email, (web)hosting, websites, domain names, in situation where the user of the (free) service is confronted with service level agreements that he or she has no influence over. This is most likely no different when (employees of) larger organisations use free of use services like Google Docs, Dropbox, WeTransfer, etc. or use cloud services from Microsoft or Amazon as a whole.

4.5. Governments

As has been shown, a government is not a unitary body. Therefore, several roles have been identified for different parts of the government.

Governments and parliamentarians have been mentioned before. They have a crucial role to play. However, this role can only start when both understand the importance of the topic. That securing the internet is a pivotal part of securing society as a whole and all its individual parts, so that the internet becomes more trustworthy and the economic, cultural, financial, etc., driver and enabler it will become even more in the future. The moment governments understand the importance of deployment, their roles will become clear as well, including partnerships to strike with other relevant stakeholders.

This report sees the role of a government from a few angles. Potential legislator, customer, policy maker, stimulator, regulator and educator. In each role a government can play a decisive role, both positive and negative, where deployment of internet standards is concerned.

4.5.1. Regulators

A regulator in this context is seen as an organisation, usually semi-independent from the executive body, charged with the role to enforce certain legislation. As far as could be ascertained at this point, regulators do not have a role in internet standards deployment, as these standards are not part of current legislation. Where this may change in the foreseeable future is the Internet of Things. However, if deployment of standards is seen as important, it is worthwhile to establish whether current legislation allows regulators to step in and enforce deployment. If so, it may be the easiest route to deployment and a more secure internet.

4.6. Consumer organisations

A consumer organisation represents consumer interests and judges the quality of products and services. These organisations can have an impact on image forming of products and brands. There soon may hardly be any products left that come unchipped into the home, public and workspace.

Especially for the ones connecting to the internet additional testing could be called for. It is in the interest of the consumer that products are safe, that his privacy is secure, his device is his and not unwittingly in the possession of a third party aiming to hurt others and / or syphoning off privacy sensitive data without consent. By scoring the digital components along with the overall quality and user friendliness, consumer organisations around the globe could influence debates on cyber security and make industry aware of its obligation to secure customers in the digital realm, e.g. through the deployment of internet standards. Just like they do in the analogue part of the world.

4.7. Internet resource organisations

In 'The public core of the internet'[54] de Wetenschappelijke Raad voor het Regeringsbeleid (The Netherlands Scientific Council for Government Policy, WRR) identified several organisations that play a vital role in the dissemination of internet resources, i.e. domain names, internet addresses and autonomous numbers (in our context DNSSEC, RPKI). None of these organisations have tools to retract these resources when abused or otherwise used in wrong ways. For many and understandable reasons, e.g. potential harm to third parties, liability, reputation, etc.

To compare, when, among other tasks, the erstwhile OPTA, the independent post and telecommunication authority in The Netherlands, in the 00s wanted to (have) shut down mobile telephone numbers that were solely abused by scamming spammers ("SMS fraud"), it found it did not have these powers. Despite being the organisation, by law, distributing phone numbers. So wished this could be turned into law.

This is different for internet resource organisations. They are membership driven and policy is conceived by consensus. History shows that it is hard to derive at a supported policy against abuse. It is here where the technical community and legislators can meet and assist each other. No matter how high the obstacles, all internet resource organisations are in a position to work in support of and are a part of the public core of the internet. Not just for distribution but also active protection against abuse. It is worthwhile considering on how to continue with this train of thought. Interaction with law enforcement has become normal in the past decade. The next step could be legislators. But for now, the focus will be on the internet resource organisations.

These are ICANN, and "lower ranked" organisations responsible for domain name dissemination and registration and the five Regional Internet Registries and their respective member organisations responsible for the dissemination of IP addresses. They have unique positions in the internet world as they have a clear public function: the dissemination of uniquely identifying resources. i.e. domain names and IP addresses. A function that ceteris paribus without the liberalisation of the telecommunication market would have fallen to governments.

The public functions of governments cannot and should not become a task of these organisations. At the same time, it is of the essence to protect the public core of the internet from abuse. There is a role to play for internet resource organisations. One they have taken up actively: they advocate internet standards actively, although mostly within their own respective communities.

[54] The Public Core of the internet, WRR, The Hague 2015

Ideally this is to change and become broader. How? That needs to be worked out further, but it involves interaction between stakeholders from the technical community, legislators and industry. Why? There is a need to establish how abuse of resources can be tackled, either by internet resource organisations themselves, with or without aid from governments. Or should there be a role for governments / law enforcement / regulators with assistance from resource organisations? How can reach out be broadened more effectively so other communities become aware of the need to deploy standards? Just some questions to start the debate with, that need an answer.

4.8. Educational organisations

Although several participants have stressed that schools from elementary level onwards should have cyber security on the curriculum, this report focusses on vocational training to university level and the need to better the offer on internet standards, security and internet architecture in general. This needs to be brought to a level that students leave their education having a fundamental grasp of how to build secure websites, software, protect information and the fundamentals of the internet, etc.

4.9. (End) users / Customers

As stated, governments and industry focus primarily on the end user where cyber security is concerned. This report does not, as the end user has a small role in deployment itself. At best as the driver of demand.

4.10. Who has what role to play?

The answer to this question is as simple as it is complex: everybody involved has a role to play. When all is said and done though, this is what remains: the organisations who have to take action. I.e. those that need to deploy. It is a diverse set of organisations, to be for sure. Internet organisations, ICT organisations, internet (related) platforms, hosting and cloud providers, domain name holders, IoT device manufacturers, ISPs, website builders and owners, school and university boards, etc., etc., etc. Only they can deploy or actively disseminate these standards and no one else.

With the identification of key players, pressure points can be identified that will allow the topic of deployment come out into the open at different levels and organisations. This will be elaborated on later.

5. Research methods

This chapter shows the strategies that have been used to get from a broad research question to a specific set of recommendations. Firstly, the goals of the research will be established.

5.1. Goals

The broad goal of this project is to find ways forward to speed up the deployment of internet standards. This goal has been specified in four smaller goals:

1. Determining the causes of slow deployment. Any search for solutions will be futile if there is no clear analysis of the problem;
2. Bringing different, and new, stakeholders to the discussion. The IGF is based on a multi-stakeholder structure. This made it important to see if there are stakeholders that are currently not part of the discussion and get them involved in the IGF. Think of parliamentarians, policy makers, industry representatives, the technical community, consumer organisations;
3. Formulate practical recommendations. This should not stay a philosophical debate. The world needs solutions and can't wait much longer in making the first steps;
4. To actively share the experiences and recommendations that have been found. This report should not end up on a shelf. Dissemination will make sure the recommendations are noticed and actions started.

Due to time and budgetary restraints not all the goals could be fulfilled to the desired level, but important steps have been taken in all aspects.

5.2. Standards used

The following internet standards were used as examples for this project[55]. DNSSEC, RPKI, bcp38, OWASP top 10, ISO 27001 and the principles of the Safe Software Alliance. The more detailed explanations of the standards can be found in Annex 3, but the most important thing now is to understand that these standards include very different ideas of the word 'standard'. DNSSEC, RPKI and BCP38 are internet standards in the technical sense. They are presented to the world in a RFC, a Request For Comments. Although generally called an internet standard, the technical community drafting the RFC in general speaks of a RFC. They form part of the internet infrastructure by providing the standardisation through which the internet works. Then there is the OWASP top 10 for websites, ISO 27001 for information security and the Safe Software Principles which basically tries at an organisational level to prevent companies from producing flaws in their software. That could be through just making the information on flaws available or providing a guide / certification for a management system that makes sure flaws are found in time.

[55] As already explained, the usual meaning of the term has been broadened for ease of use

5.3. Identify causes and directions for solutions

This project started with drafting questions for a survey that was disseminated in cooperation with many and different internet (related) organisations from around the globe. The provided answers made it possible to propose five concept recommendations which were used to conduct further research. Online research was done to learn more about initiatives and find other information that was all tested and discussed in five break-out groups at the IGF workshop and in the interviews.

5.3.1. Dissemination of survey

Several local, regional and global organisations showed their willingness to assist in the dissemination[56]. In practice it proved hard to do in the summer of the northern hemisphere. This led to an extension of the final date with one month, leaving too little time to have all data thoroughly analysed before the IGF. In all honesty, the response remained lower than hoped for. This did not stand in the way of distilling concept recommendations, as those responding, from around the globe, clearly pointed in very specific directions.

5.3.2. Survey response

Even though the numbers were low, enough people seemed to agree about answers, that were tested in the workshop and followed up in the interviews. People who participated in this project either by being interviewed or otherwise and who are knowledgeable about the topic, tend to think along the same lines, despite not agreeing on the desirability of each specific outcome. The recommendations are more or less agreed upon as potential outcomes as the basis for further work.

5.4. Getting different stakeholders into the discussion

One of the aims of this project was to reach out to stakeholders who are not overly familiar with internet standards and underrepresented at the IGF: parliamentarians. A special program was conducted by the host country, where this project was able to feature in as an urgent example for the need for parliamentary participation.

5.4.1. Outreach to parliamentarians

A part of this project was aimed at reaching out to parliamentarians and explain to them how important it is for them to understand the deep and profound ways the internet and ICTs change the way we live, work, rest and play[57]. These changes not only have an impact on society as a whole but more specifically on their respective fields of expertise. Whether parliamentarians have health,

[56] See annex 1

[57] Yes, this is a deliberate quote from a The Undertones song about a certain candy bar.

agriculture, jurisdiction, mobility or sports as expertise, they need to understand that internet, ICT, data, privacy, etc., have become a component of their oversight that needs to become normal to address and incorporate in their oversight and legislative actions.

5.4.2. BMWi ambition

This intention coincided with the ambition of the German IGF 2019 host, the Federal Ministry for Economic Affairs and Energy (BMWi). This led to a combination of efforts. Presentations were given to parliamentarians at the local, regional and global level in combination with an extensive outreach program on behalf of BMWi[58]. This led to circa 160 parliamentarians registering to the IGF, an absolute record and between 15 and 20 parliamentarians participating in the internet standards deployment workshop at the IGF. To attract them to the IGF the following arguments were provided[59]:

- *"Software, ICT products, code, sensors, they are found all around us and have one important thing in common: they are all connected through the Internet. Whether you specialise in health, privacy, mobility, legal, building or agriculture, ICT has become an important part of your field of expertise - knowingly and more hidden in the background. This comes with challenges and future tasks. Questions on privacy, access (to data), security, use, etc., need to be addressed and decided upon;*
- *Yes, these are extremely technical matters, but no less technical than deciding on safety measures for airplanes, cars or medical equipment. Just as standards have been developed for all critical infrastructures, they must be discussed and decided upon for our digital world as well. What we do right in the first place will help us secure sustainable growth in the next phase. Society today would not dream of letting a car on the road without breaks, safety belts nor drivers without knowing the rules. This should not be different for ICT (related) products. Currently it often is. A situation you can help change;*
- *On a more abstract level, ICTs have brought changes to diplomacy and the way state and non-state actors use and abuse the opportunities the internet currently offers. This topic comes with challenges how to deal with these actions, challenges that all politicians will come to address in the coming years through legislation, treaties, codes of conduct, etc.;*
- *Often practical solutions against abuse options already exist, but are not always voluntarily deployed by industry".*

[58] All parliamentarians were invited by way of a letter of invitation of the Bundestag president, Dr. W. Schäuble and Jimmy Schulz, chairman of the Digital Agenda Committee, to his colleague presidents and chairs and individually where possible through existing networks. Workshops were given in the German and European Parliament and at the Inter-Parliamentary Union meeting in Belgrade.

[59] A reach out work program coordinated and executed by Medienstadt Leipzig e.V. in cooperation with De Natris Consult

5.4.3. Participation parliamentarians

A first outreach session preceding this pilot project was organised at the NLIGF[60] in 2018. In this session the concept of RPKI (Resource Public Key Infrastructure) was explained to an audience including parliamentarians, consumer organisations, policy makers, industry and others. Several of the people in the room had been specifically invited to join. For many it was an introduction to the existence of this standard (and all other standards - and the (NL)IGF) and what it tries to mend, but also an insight that needed pursuing. In fact, it led to the presentation at the Inter-Parliamentary Union in 2019. Nothing changed that day where deployment as such was concerned. It indicated that there is a world to win and to make outreach to communities beyond the usual suspects a priority; if these internet standards are ever to be deployed that is.

The fact that the topic internet standard deployment was raised successfully in a national IGF, aiding in the understanding of the relevance of internet standards deployment within other stakeholder communities, should not be mistaken for failure because of a lack of (instant) success in the deployment itself. It is a first step to potential success. This insight led to the concept of identifying and naming potential pressure points in societies.

At the IGF itself many parliamentarians realised that they have a role to play. E.g., those who are technicians could act as instructors for those who are not or as digital champions.

5.5. Limitations

Not all outreach proved possible at this stage. Funding could not be found to actively engage with consumer organisations. However, initial contact showed the interest is there.

Funding as well as time restraints did not allow for the creation of online working groups preparing the IGF workshop and report.

5.6. Demarcation

To prevent misunderstandings potentially surrounding this topic, certain demarcations need to be made about this report.

1. No assessment of standards (processes)

This report does not include in any way an assessment of the standards or protocols itself, nor does it advocate this or pass judgement on the processes used to derive at a new standard. It does not aim to create any form of oversight over these processes or the organisations creating them. Later in the report recommendations will be presented on communication (channels) and the testing of new

[60] The national IGF of The Netherlands

protocols before publication, but these sub recommendations stand apart from the standardisation processes at such[61].

2. No proof of problem

This report will not argue whether the issue at hand exists or not. The attention the topic has received for many years is proof enough. Hence the report focuses primarily on potential ways forward.

3. Prevention vs. mitigation

In this report a strong partition is made concerning cyber security measures. It focuses exclusively on measures that prevent harm and abuse. It does not focus on industry mitigation programs nor on measures for end users. So e.g. you won't find botnet mitigation centres, DDoS scrub streets, Anti-Virus products, the need to update, nor training-the-public-programs in this report. (But, yes, of course they are extremely important to have but may become less so if prevention would prevail over mitigation.)

4. No binding outcomes

This report is written under the aegis of the Internet Governance Forum. Hence it does not contain in any way a negotiated decision or anything binding. Nor can it be taken as a formal IGF document. It is an advice to the MAG and the world at large. The recommendations presented below are the outcome of accumulated and aggregated views from many individuals. Many views coincided and they are presented in this report as potential ways forward, within the IGF and beyond.

5.7. Non-cooperation

Unfortunately, this report does not hold any formal input from representatives of the IETF and Internet Society. It proved they were not willing to provide input despite repeated invitations to do so. In communication with representatives, concerns were raised. This report has addressed them and hopefully succeeds in taking these concerns away, so future cooperation and exchange of ideas will become possible, as the technical community is an important factor in addressing the challenges and creating solutions.

Also, it was indicated by some that the IGF is not seen as the place to find answers to complex internet governance issues. Some indicated that the IGF is not taken seriously by our community. Another made the comment: "We do not engage with the IGF". This also led to not providing any, extremely relevant input, to the project. It is up to the IGF itself to prove those not engaging or criticising wrong.

[61] There is one exception. Where people active in IETF meetings and work commented on the process or outcome this is shown as an example for potential development and growth for the IETF itself to decide on

6. Other initiatives

The number of commissions, panels, studies, advisory committees, industry and government best practices and policy, etc., reporting on a secure internet, a trustworthy internet or more secure products are numerous and for a limited project like this impossible to fully keep track of. Let alone read them all. Norms are proposed, best practices identified, policy written, self-regulatory measures suggested, bilateral treaties signed, anti-abuse measures discussed and implemented, etc., etc. A few relevant ones to this report are presented.

6.1. The public core of the internet

The public core of the internet is a term that was the title of a study of the Dutch WRR[62] from 2015. Its purpose was to define foreign policy of the Dutch government concerning internet governance. The WRR defined the public core as follows:

"*The Internet's public core embodies a number of abstract values. Universality, interoperability, accessibility, integrity, availability and confidentiality are the core values that guarantee 'the Internet' as a global system*[63]".

In other words, they are also about the functionality of the internet. The DNS system, the routing, the integrity of data therein. It is no coincidence that some of the internet standards used as an example for this report are standards making the core of the internet work. So, what protects and upholds that core? "*The task of upholding these values and functions has been entrusted to institutions, protocols and standards*"[64]. It is safe to conclude that all these tasks lay within, what the internet governance world calls, the technical community. The conclusion that can be made is that internet standards are part of the public core of the internet in need of protection from "*improper use of this core by nation states or other entities*[65]".

The institutions mentioned, e.g. are ICANN, IETF, W3C, the RIRs, etc. So if the public core of the internet is imperative to protect, what is the reason that the standards defining the functionality of the internet are not a part of (inter)national policies and laws discussions?

6.2. Global Commission on the Stability of Cyberspace

The GCSC adopted the notion of protecting the public core of the internet. At the start of its report the Commission identified a seven element Cyberstability Framework. The seventh element underscores the importance of this pilot's work: "*(7) the open promulgation and widespread use of*

[62] The English version can be downloaded here: https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet
[63] The Public Core of the internet, WRR, The Hague 2015, page 45
[64] Idem
[65] Idem, back cover

technical standards that ensure cyberspace is resilient”[66]. Something which lies at the heart of the public core of the internet. It came as a surprise that this specific topic was not pursued further by the GCSC. This has been attributed to a lack of time and feeling of urgency. Despite this, one of its recommendations underscored what many respondents to our survey derived at: ”*States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene*”[67]. Ideally “our” standards become a part of this discussion, but reading the text on this recommendation, it is noted that the technical internet standards are not mentioned, not even as an example[68].

Quoting this text from the Commission’s report, gives rise for the need to start including internet standards and look beyond the formally recognised standards bodies:

> *“To this end, the Commission strongly endorses the widespread adoption and verified implementation of basic cyber hygiene—a regime of foundational measures that represent prioritized, essential tasks to perform to defend against, prevent and rapidly mitigate avoidable dangers in cyberspace”*[69].

Again, it looks like internet standards fell from an agenda and an opportunity to start a serious discussion was missed. The topic was brought in by a commissioner from the technical community, but not picked up. This leads to some questions that will come back later. The following may be a start to provide an answer to why internet standards are not seen as important enough to work on within a commission like the GCSC.

6.3. The Paris Call for trust and security in cyberspace

The Call published during the IGF in Paris in 2018 holds many norms that are at the basis of the work on, research for and cause of this report, including protecting the public core of the internet. Notably, the deployment of internet standards is not mentioned as a possible solution, despite the fact that deployment would contribute significantly to positive outcomes for the Call. Strengthening the security of digital processes, products and services is[70]. Potential steps forward will be presented below.

6.4. Hague Centre for Strategic Studies

When Under-Secretary-General Fabrizio Hochschild mentioned in one of his contributions at the IGF that it was time someone brought the reports of all the initiatives together, he most likely was unaware that this initiative had already been carried out in The Hague. As was already shown, the

[66] Advancing Cyberstability. Global Commission on the Stability of Cyberspace November 2019, page 8 https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf
[67] Idem, page 9
[68] Idem, page 43
[69] Idem
[70] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

HCSS has built a tool in which 900 cyber (related) norms have been brought together and analysed as a part of the GCSC's work on norms.

6.5. Deploy 360

The Internet Society worked on a program called Deploy 360. With a similar aim to this project: "implementation of new technologies and standards"[71]. From the information that has been found online there are two differences between Deploy 360 and this project. First, Deploy 360 aims primarily on IETF standards and primarily focuses on the technical community and industry. Under the program best practices were gathered, studies explaining deployment written and conferences organised where the people who physically have to deploy the standards are connected to and instructed by early adopters.

There is a second difference between the two programs: to involve stakeholders beyond the technical community to make them understand the importance of deploying said internet standards. They may be able, from their respective places of influence, to apply pressure on those in the decision seats who decide on creating the financial wherewithal to deploy. 'Am I speaking to the right person?' is an important question to keep asking.

In a private email it was explained that Deploy 360 was met with "mixed results". As has been mentioned before, ISOC chose not to interact with this IGF pilot project, hence this report is not able to learn from the lessons of Deploy 360. The interest to learn more and if possible, integrate our respective knowledge and experience in 2020, e.g. through the Open Standards Everywhere Project that was announced recently[72], is there. Especially since the goal of this report seems to be the same: internet standards deployment.

6.6. MANRS

MANRS stands for Mutually Agreed Norms for Routing Security (MANRS). It is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats[73]. Among others, the observatory shows how slowly the RPKI standards is deployed around the globe[74].

[71] https://www.internetsociety.org/deploy360/ (accessed 23-12-2019).

[72] On finalizing this report, we received news that ISOC had started a new program: 'Introducing our Open Standards Everywhere project – securing web servers in 2020!' with the following goal: "*By the end of 2020, our goal is to see an increase in security and availability of web servers across the Internet through the usage of TLS, DNSSEC, IPv6, and HTTP/2*". See: https://www.internetsociety.org/blog/2020/01/introducing-our-open-standards-everywhere-project-securing-web-servers-in-2020/ (accessed 02-02-2020). Let's work together in 2020.

[73] https://www.manrs.org/ (accessed 20-01-2020).

[74] https://observatory.manrs.org/#/overview (accessed 2-01-2020).

7. Conclusions

The combined efforts conducted within the project led to several, very different insights. In fact, many reasons for slow deployment were presented.

1) There is a lack of a (positive) business case.

2) There are hardly any other incentives supporting voluntary deployment.

3) Some standards may not be good enough as they do not get deployed or are (too) difficult to deploy.

4) The dissemination of the standards could be better. Both in “translation” of the necessary actions and the reasons for and reasoning behind the standards and in the actual proliferation of the standards after publication.

5) There is a need for interaction, even collaboration between the technical community and policy makers and civil society, e.g. by way of a consultation phase.

6) Many trade organisations, companies and especially SMEs are not involved in the standardisation processes and / or less active within trade organisations so may never have heard of these standards.

7) There is a need to change the narrative concerning internet standards (and cyber security in general) to reach management, owners and boards deciding on the investment.

8) There most likely is a lack of technical knowledge and / or resources to actually implement the standards within SMEs and perhaps some bigger companies as well.

9) Education curricula do not provide the necessary knowledge concerning internet security and governance.

Many different initiatives have been identified as were proposed ways forward. In this chapter they are presented, and conclusions provided.

Subset 1: The stimulation of a business case

Many participants pointed to the fact that there is a lack of a (positive) business case. What could change this?

7.1. Financial Stimulus

SIDN, the .nl registry, in 2019 is the world leader where signed domain names is concerned. 54% of the domain names is signed[75]. SIDN offers all domain name holders who signed their domain name a discount. Although on the one hand it can be said that still 46% has not deployed DNSSEC yet, .NL is global leader through this financial stimulant. Last July it has extended this program to DANE (DNS-based Authentication of Named Entities), a protocol for the secure publication of public keys and certificates that builds on the deployment of DNSSEC[76].

Taking precautions, deploying standards, building security into services and products costs money, money industry must be able to make a return on.

Financial stimulation proves to be a pressure point as it creates attention to the topic and adds a positive business incentive attainable for all.

7.2. Internet security and cost for business

In countries where the telecommunication market was liberalised governments lost any say about the use of networks and company investment. With the roll out of the internet and all its institutions, standards and services, there was no role for the government at all. The internet is “ruled” by consensus from those actively participating in these meetings and the measures agreed upon are solely voluntary to deploy.

Government involvement or interference where the deployment of internet standards is concerned, leads to administrative costs. This appears to be one reason why government interference with internet and ICT (related) products is at a minimum. This text in the NIS Directive points towards this conclusion:

> “*To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the*

[75] SIDN stands for Stichting Internet Domein Namen. https://www.sidn.nl/nieuws-en-blogs/nieuwe-stimulans-voor-beveiligingsstandaarden-dnssec-en-dane (accessed 12-12-2019)

[76] It is however necessary to put the result of SIDN into perspective. APNIC, the Regional IP address organisation of the Asia-Pacific region, scores the DNSSEC deployment for the whole world. In The Netherlands only 21.26% of the domain names is validated, 25,62% partially validated, putting the .NL domain at a low level across the world. The absolute number of (partially) validated domain names with 865.050 can be called high, as .nl is one of the largest top level domain names in the world (https://stats.labs.apnic.net/dnssec Stats for 18-11-2019 till 17-12-2019 (accessed 18-12-2019)). Compared to the number one spot, Saudi Arabia, with 99.24% or number 5 Iceland with 98,21% , .nl scores low. It would be of interest to learn why these two, very different countries both score this high.
We have not found a final answer but have been pointed to the following. In Saudi Arabia all internet traffic is monitored at a single point of entry. If this point is validated, all traffic appears to be validated. It does not say anything about the organisations behind the point of entry. Iceland only has a few ISPs. If they have all validated their domain, the score is near 100%.

> *state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises*"[77].

Looking at internet security measures only as administrative costs for industry contributes to the negative level playing field and is a cause of non-deployment.

7.3. Government procurement

A way to create a positive business case is by leading by example[78], e.g. through procurement. Governments should function as a role model and a supercharger in the implementation of internet standards, by practicing what they preach. When a government (or large enterprises for that matter) deploys or demands these standards, it can take away some of the first-mover disadvantages for private sector players. To include security standards as a prerequisite to public procurements, it provides industry with a clear advantage to implement the standards. This will lead to trickle-down-affects others profit from.

One example is the work of the Standardisation Forum (Forum Standaardisatie) in The Netherlands. It has drafted a list of 42 open standards all government bodies in The Netherlands have to ask for when procuring over € 50.000, - or explain in a serious way why they do not deploy ("pas-toe-of-leg-uit")[79].

The EU has a similar initiative supporting open standards in the form of a Commission Implementing Decision on the identification of ICT Technical Specifications for referencing in public procurement[80]. Lemma 4 recognises non-official standardisation bodies explicitly: "*the most relevant and most widely accepted ICT technical specifications issued by organisations that are not European, international or national standardisation organisations*"[81]. This is a significant step towards voluntary deployment by governments, creating the much-needed business case through active procurement and setting standards for industry to follow.

Government (and large corporations) can use their procurement powers to assist their suppliers to build in security measures into their respective products and services. This will most likely lead to the new standard of their product. This is an, economic, pressure point.

Active awareness campaigns on the benefits of security measures, outside of the usual channels, are another identified pressure point.

[77] NIS Directive, page 8

[78] See e.g. the Dutch government consultation on making the deployment of standards mandatory for itself: https://www.internetconsultatie.nl/overheidswebsites

[79] https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit (accessed 12-12-2019)

[80] COMMISSION IMPLEMENTING DECISION (EU) 2017/2288 of 11 December 2018 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D2288&from=EN

[81] Idem

Subset 2: The pros and cons of legislation and regulation

"If tech executives want to change, there's no need to wait for government regulation to guide them in the right direction"[82]*.*

7.4. Legislation

Legislation is being named as a possibility in ensuring the implementation of internet standards. In fact, of the recommendations provided in the survey, it comes forward as the only measure that will ensure deployment. Or, as the participants in the break-out session on secure products by design indicated, they seriously doubt whether industry will ever self-regulate to the level necessary and called for certification backed by a law.

At this point, based on the data available to us, internet standards are not part of laws and regulation. It is impossible and most likely untrue to state the non-deployment of standards is caused by the lack of laws, but it certainly does not help. Why?

There is no doubt legislation would create the level playing field called for, as it provides the comfort to deploy in the knowledge competitors will deploy or suffer the consequences if they don't. Also there is no need to create a business case or draw customer demand, neither is a discretionary decision by management required. As such, reading all the other options and taking in the tremendous effort these options will take to become a success, if ever they do, legislation is the shortest route to deployment.

However, legislation also appears to be the least favourite option of nearly everybody, including policy makers and parliamentarians. Many pointed to the fact that the technical advancements move so rapidly that a law always runs behind, besides the risk that it will slow down the process of making the internet more secure. Others doubted whether a law can ever actively respond, as in adding standards modified or released after the codification of the law. An internet technician provides the following warning: "If internet standards must become law, then never mention individual standards". This point of view was shared by representatives from other stakeholder groups. A law would have to be made generic, so adaptable to future changes. However, the present front page of IETF shows the following news:

> *"Providers of voice over IP in the United States will be required to implement the IETF's Secure Telephony Identity Revisited (STIR) protocol as a result of recently enacted legislation to address some of the root causes of illegal robocalling on the telephone network"*[83].

So, an RFC can be turned into law when a government deems a case too pressing or damaging. The origin for the law lies in the explosive growth of robocalls, notes the IETF website. It would be interesting to learn what makes this topic different for the U.S. government from other forms of internet standards concerning internet abuse and crimes. The Federal Trade Commission, who

[82] Big Tech companies want to act like governments, Marietje Schaake, Financial Times, 20-02-2020
[83] https://ietf.org/blog/stir-action/ (accessed 20-01-2020).

regulates the law, states that the fact that most robocalls are scams is the motivation behind the law[84]. This motivation could be an opening for further legislation it seems.

7.4.1. The EU and standards in general

In his book 'The New Approach To Technical Harmonisation and Standardisation'[85], Pelkmans shows how standards were built into the fabric of EEC trade and became a fundament under goods getting free access to markets. He stresses that although the standards are voluntary to adopt, each manufacturer or trader has to show he complies with the standards, in order to gain access to the internal market. Again, the standards pointed to are set by official standard bodies, e.g. CEN and CENELEC. However, it is this quote that could provide a potential way forward, if internet standards are to become recognised as standards: *"It is the task of competent (private) standardisation organs, given technical progress, to formulate the technical specifications, on the basis of which industry needs to manufacture and market products complying with the fundamental requirements of the Directives"*[86]. It is worthwhile for governments and the European Commission to develop this idea further, like e.g. is currently negotiated under the Radio Equipment Directive.

7.4.2. Examples of current law

The lack of a carrot and a stick is underscored in the already mentioned NIST and Australian communications, the NIS Directive of the EU and the conclusions of the HCSS tool.

This leads to the conclusion that internet standards as described here, at a minimum in the European Union, are not part of formal political debate and decision making. For the internet to become more secure a question needs to be asked and at some point in time answered: Is this a satisfactory outcome and the desirable way to progress?

This is no different where certification on Internet of Things devices is concerned. Although the Cyber Security Directive contains certification as an indication, it is currently not mandatory to implement. *"The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures"*[87], the Commission writes. This harmonisation process of current certification schemes is under way and a commission of experts has been established[88]. An assessment of certification schemes by the Commission and whether to impose them will not take place before 2023[89].

[84] https://www.consumer.ftc.gov/articles/0259-robocalls (accessed 14-02-2020)
[85] The New Approach To Technical Harmonisation and Standardisation', Jacques Pelkmans. Journal of Common Market Studies Volume XXV, Nr 3 March 1987
[86] Pelkmans, page 255 (The Directives mentioned are those made under article 100 of the EEC Treaty.)
[87] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (accessed 12-12-2019).
[88] Ibid.
[89] https://www.nen.nl/Normontwikkeling/Doe-mee/Normcommissies-en-nieuwe-trajecten/Cyber-security-en-gegevensbescherming-1/IoT-vraagt-om-standaarden.htm.

The U.K. has met with government representatives of Australia, Canada, New Zealand and the United Stated “*to discuss our common security challenges with regards to the Internet of Things (loT), and how we can best protect our citizens from cyber threats*”[90]. It is acknowledged that no single country can deal with this topic individually and that it can’t reach success without an effort, voluntarily or through certification, *from industry*[91] (italics WdN).

Consumer law does not assist either. In EU legislation consumer law is being redefined for the digital age. The right to security updates for a period of time that is seen as reasonable for digital services, games and products with digital components, e.g. smart TVs, becomes the norm: “*For the period of time that the consumer would reasonably expect, the trader should provide the consumer with updates, including security updates, in order to keep the digital content or digital service in conformity and secure*”[92]. That the harmonisation of the internal market is used as the reason for this feature in the directive is not important. Consumers have a right to claim secure products and remain or made more secure as time passes. It must be noted that this is not a cyber security directive but a consumer protection one. The question to ask is whether this is the direction needed. Again, it seems E.U. governments are about to lay the responsibility of securing devices and thus society in the hands of those least competent and powerful: the end user. In the U.S. they do to. Shouldn’t the following question be added: What period of time is reasonable for society at large to be provided with updates by the trader for devices hooked up to and accessible through the internet?

There is another consumer law angle. The NIS Directive of the European Union does not go further than mentioning hard and software in the sense that these “products are already subject to existing rules on product liability”[93]. With lemma 51 it even goes a step further by excluding interference with the quality of products:

> *”Technical and organisational measures imposed on operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner”*[94].

This is more or less in line with the NIST website communication referred to before. The question is, is this enough? When reading terms of use of software and (free) internet services, the liability for using the software and service usually lies with the user. The NIS Directive sees the user of the software or service in a traditional customer - vendor relationship, whereas the internet industry often looks at customers primarily as users, especially when offering free products, where the user is the real product. So, does the NIS Directive solve what it aims to solve where cyber security and creating more secure soft and hardware is concerned? This report declares it does not.

[90] https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things.

[91] Ibid.

[92] Article 8.2.a DIRECTIVE (EU) 2019/770 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, page 9

[93] EU NIS Directive, page 8

[94] Ibid.

It is safe to conclude that the standards mentioned in laws are not the same as the internet standards produced by IETF, OWASP and safer software initiatives. If these standards are to be deployed more swiftly, this needs to change.

Currently internet standards are a part of debate in the preparation of a new directive. We return to this below.

Finland

There is, as far as this research has been able to find, one clear past example of how legislation can work. The example as such falls outside of the scope of this report, as it is about botnet mitigation. It is presented here, as it is a use case. Finland traditionally scores the lowest in botnet infections for over a decade. In 2006 it became law for ISPs and telco's, after notification by the regulator, to disinfect the device of an end user within a limited number of hours[95]. In how far this has the additional benefit of being less attacked, is unknown, but is imaginable. Why target a country where the rate of success is extremely slim? With the, voluntary, Abuse Hub function in place, The Netherlands scores quite good as well[96]. Although botnet mitigation is not the same as internet standard deployment, it may be possible to find answers here to the questions asked in the next paragraph.

7.4.3. Taking the easy way out?

Legislating deployment of internet standards is beyond doubt the easiest way to ensure a more secure internet. All other options cost more time, effort and relies fully on the well-meaning of many involved stakeholders. As such legislation is one of the recommendations of this report. However, as legislating deployment is not desirable, at a minimum the world must know why this is and whether it is for the right reasons. Some questions need a clear answer. The following are just examples to start the discussion:

- Would legislation make deployment harder?
- How can legislation be written without hampering deployment?
- In what way would legislation alter the development of the internet?
- Would legislation make permissionless innovation harder / impossible?
- Would legislation change or stop IETF, W3C, OWASP, etc. activities?
- Is there another way to create a level playing field and if so what?
- Can legislation follow developments without causing endless delays?

[95] In this report background information is shared by the Finnish regulator FICORA (since 1-1-2019 Traficom) http://www.cert.fi/en/reports/2012/information_security_review_1-2012/dnschanger.html

[96] Zero Botnets. Building A Global Effort to Clean Up The Internet', Jason Healey and Robert K. Knake. Council of Foreign Relations, November 2018

- Can legislation be written technology / standard neutral?
- Must internet standards be identified at the same level as current standards in laws?
- What makes the internet and ICT different from other, regulated industries?

These questions are in need of an answer in order to make a sound decision on whether legislation is truly undesirable as a solution for deployment or that it is an option after all. At this point it is too early to be able to tell.

Without a doubt legislation is a major pressure point.

7.4.4. Interaction

There is an urgent need for interaction between different stakeholder communities; if these standards are to be deployed in a swift manner. If the technical, industry and policy making communities were more forthcoming in their contact, this would make the internet standards, procedures and their desired outcomes more widely known. For internet standards deployment to become the standard, this has to change in the future. It is here that the IGF, as a neutral, global, but involved organisation can play an important role and bring the stakeholder groups together and discuss future interaction, collaboration and dissemination.

7.4.5. Regulation

Legislation alone would not be sufficient. In the following, two different ways to look at regulation for securing the deployment of internet standards are presented.

Option 1. A new law

If internet standard deployment is written into law by reference, it needs a strong (independent) regulator that is able to enforce deployment by those who do not or insufficiently comply with the law, thus breaking the necessary level playing field. Although Politico recently declared GDPR regulation a near toothless tiger[97], it is a good question whether other now successful regulators were so in the first two years of existence. Several organisations around the globe charged with the enforcement of unsolicited communication ("spam"), were quite successful in the 00s. Funding and the right staffing is an important if not decisive factor for successful regulatory actions.

The power of the regulator is a necessary part of a law that would make deployment mandatory by reference. Without it there remains no stick.

[97] ''We have a huge problem': European tech regulator despairs over lack of enforcement'. https://www-politico-com.cdn.ampproject.org/c/s/www.politico.com/amp/news/2019/12/27/europe-gdpr-technology-regulation-089605 (accessed, 10-01-2020)

Option 2. Current laws

It is also possible to look at regulation from another angle. One that at this point in time comes with more questions than answers, but, if possible, would need no "deployment law". So, what could be options to study further?

Regulation comes in the form of fines and / or other forms of pressure from laws. What is an interesting thought is to establish whether current laws can achieve deployment. It would come as a surprise if one of these laws currently would mention internet standards. So, the question lying in front of us is, what provisions already are part of e.g. telecommunication, privacy, finance, consumer protection, civil, cyber security, etc., laws? In other words, is there a formulation in current laws that can be used to make deployment mandatory? Can non-deployment of certain standards lead to a (higher) fine, because of negligence, liability, duty of care, privacy violations, etc.? Duty of care is already common in several laws. Does refraining from protecting end users from cyber harm through non-deployment constitute non-compliance with a duty of care? Can regulators be tasked to compare operators, hosting providers, websites, internet services, platforms, etc., on the deployment of standards, etc., like e.g. a consumer organisation would do for products or services[98]? Perhaps there are even grounds to work together here. This may be a new role for some, but worthwhile exploring; if legislation is considered out of order. The questions posed here are all in need of answering.

As an example. In Europe the General Data Protection Regulation (GDPR) has become the norm in privacy. As such the directive does not make any statement about internet standards. It does say the following in article 2.f:

> *"(Personal data shall be:) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"*[99].

Could this give rise to demand certain standards to be deployed or give rise to demand safe IoT devices and software to be purchased? Another question in need of an answer.

Regulation is an identified pressure point.

7.4.6. The U.K.

It was pointed out by a parliamentary participant in the Berlin IGF workshop that the United Kingdom was looking into whether OFCOM, the Office of Communications, is to regulate internet standards, something several representatives from African countries suggested was an option for their countries as well. This could be an interesting way to pursue thinking about deployment for more countries.

[98] The Dutch Agentschap Telecom (Radiotelecommunications Agency) has started a program on securing IoT devices

[99] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

7.4.7. Penal code

For the bad actors who do not deploy or comply in any way, most likely other laws are applicable to their misdeeds, e.g. the penal code or a telecommunication act. To identify truly bad actors more easily, all others must start deploying.

7.4.8. Summing up

So, to conclude. At this point in time, on the basis of information available, internet standards are not a part of legislation and regulation. At best it is found in consumer law and even then, in the relationship between manufacturer and / or retailer and the customer. However, if legislation is to be considered, there is a near unanimity that it needs to be a last resort.

This report disagrees; <u>at this point in time</u>. It gives the recommendation to research the topic further to be able to come to a sound conclusion. E.g. to make an inventory of the arguments against legislation and test them. And, if legislation (and regulation) is the last resort, there may be a need to prepare work on it, as a contingency plan for when all else has failed. This would provide all concerned a clear-cut result of the consequences of non-deployment. The absence of legislation must never equal non deployment; as it does now. A way forward is to work together on this contingency plan. For policy, technical community and industry representatives there is no alternative to learn each other’s points of view and learn from each other.

Legislation, together with the option to regulate, is identified as the most major pressure point society can apply.

7.4.9. Role of government in other sectors

Risking the comments that are usually proffered where comparisons are concerned, it does make sense for policy makers and parliamentarians to look at other industries and compare how they are regulated to ensure security, safety or health standards. The internet can be seen as the road or the sky and the products as the cars or airplanes. There are rules of the road that everyone needs to adhere to and when caught in breach of the law is fined or worse, while cars and planes have all sorts of standards that need to be built in.

This insight leads to questions in need of an answer. In what way are the internet and ICT (related) products different from other industries? And if so, does this make it impossible for parts of the internet and ICT (related) products to be regulated? And if the imposition of standards or certification is seen as necessary, is this an administrative burden or a necessity to behave as a sensible, responsible manufacturer or service provider? Answering these questions will add to the ones asked about legislation.

It is suggested to look at the topic of deployment as a digital health issue. This can sharpen the minds on who needs to act and in what way.

When policy makers and parliamentarians invite the technical community and industry to address and answer these questions together, another pressure point is identified.

7.4.10. Government pressure

Several participants pointed out that governments can put pressure on industry by discussing deployment pro-actively, by showing the importance they give the topic. Parliamentarians could champion certain standards. Because of consolidation, more and more parts of the internet, horizontally and vertically, come into the hands of a few players, as the winning platforms tend to grow larger. Despite the fact this makes those players as a whole more powerful, there are also less organisations to address where deployment is concerned. It was also pointed out that the business model of these platforms prevents them from deploying certain internet standards. This comment needs further research, to make it more substantial. However, if these organisations can be convinced to lead, the internet would be safer for many instantly.

The necessity to do so is shown in the testing results the Dutch Standardisation Forum presents in a report from 2019. The signing of DNSSEC and the use of DANE recently went down in The Netherlands due to the fact that provincial and local governments started using Microsoft Office 365 Exchange Online. This service does not support both mentioned open standards[100], making Dutch society less secure than it was before.

That a large platform, Office 365, can change, comes forward in a report following a privacy assessment. Microsoft mitigated privacy risks in its relation to the Dutch government. The fact it had to, shows two things: the first is the way Microsoft gathers data through this service, the second how government pressure can lead to change[101].

By addressing the topic of deployment, governments and parliamentarians can apply pressure to platforms and industry.

Subset 3: Security by design / default

7.5. Written into standards

Several participants pointed out that current standards do not have any practicality nor a business case in mind. They can be unpractical as there is no incentive provided. This was pointed out in different wordings throughout this report, but pointing to the same outcome. Several participants pointed to a specific part of IETF's procedures. (Participants in) the IETF have a much wider role than may be acknowledged at this point in time. Internet standards are not just written to make the internet function better, they have policy, political, financial and educational implications. As such, standards need to reflect these implications, as the outcome of an IETF process has implications for society at large. Making the internet a safer and more secure place is an important task of all

[100] Meting Informatieveiligheidstandaarden september 2019. Forum Standaardisatie, September 2019

[101] Chapter 17. Risk mitigation measures, in 'DPIA Office 365 ProPlus version 1905', p 105-106. Sjoera Nas, Floor Terra, 22 June 2019.

standard bodies. As a reminder, as was mentioned before, all the people that interacted with this research only pointed to IETF, but there are more standard bodies involved. The deployment of the standards is an important part of the work to be carried out. Including the societal implications of security related internet standards, it becomes of importance to determine how standards, once validated by the members, can be deployed in the swiftest of manners. It was suggested to take this challenge into consideration during the drafting process. Where possible internet, security related standards have to be written with a level playing field in mind, e.g. a stimulant like a positive business case or a forceful incentive worked into it.

This is something IETF sees as a core function. The following text comes from the IETF website:

> *"In outline, the process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body... and is published. In practice, the process is more complicated, due to (1) the difficulty of creating specifications of high technical quality; (2) the need to consider the interests of all of the affected parties; (3) the importance of establishing widespread community consensus; and (4) the difficulty of evaluating the utility of a particular specification for the Internet community.*

The goals of the Internet Standards Process are:

- *technical excellence;*
- *prior implementation and testing;*
- *clear, concise, and easily understood documentation;*
- *openness and fairness; and*
- *timeliness.*[102]*"*

The disparity between the comments received and this quote leaves us with the question that when IETF has these principles as an outline, how come several participating in the IETF point to the fact that IETF needs to do more? Due to the non-cooperation further research at this point was constrained. The recommendations will address the topic further.

7.6. Internet of Things: Security by design / default

The Internet of Things "is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction"[103]*.*

[102] RC 2026 and https://ietf.org/standards/process/ (accessed 2-1-2020)

[103] Wikipedia (accessed 12-12-2019)

It seems that as a standard many ICT (related) products come onto the market without a baseline of security, thus defence in place. Security does not even come as an afterthought, it often seems not part of the product. Connectivity is. For a host of reasons, but very often to gain data on the user of a device and / or to service and monitor it.

This lapse of security puts others at risk. Spying, hacking, the loss or manipulation of data and privacy, etc., all become possible because a lack of basic security built into a device. Next to abuse of other forms when the device is used to attack on other entities, e.g. through a DDoS attack, spam or malware distribution.

At this point in time, there is not a sufficient business case for raising security. There is carrot nor stick. For this to change, the barrier needs to go up.

It was pointed out that a one size fits all strategy may not work. A complex machine like a F35 fighter plane or a car, both filled with software and a single chip in a toy cannot be treated in the same way. So a layered approached may be called for. Still it goes without saying that no security on countless millions of cheap chips leaves the world totally vulnerable. Where the bottom line lies for each category is for governments and / or codes of conduct to decide. The current approach calls for voluntary action. This is not enough. There have to be incentives to change and that starts e.g. with procurement by governments and large corporations. They create a market. To cater it manufacturers will build in security by design.

Even if voluntary action is the way forward, governments will have to deliver input about what is a desirable level of security and the level and length of repair / mitigation. How many updates are called for? What is a suitable time frame for updates compared to the life cycle of a product? What is a baseline protection? What happens when a supplier of software in the product of another company goes bankrupt or stops activities? Are rights transferred when the product is sold to another person (in another country)? What is a baseline before code can be released in a product? Just a few of many questions in need of an answer that governments may want to form an opinion on before agreeing to voluntary industry standards.

A second way forward is stricter. Governments formulate the baseline of security through a certification or a code of conduct. If this comes with the choice to self-regulate and make deployment of standards voluntary, there needs to be a plan b formulated for those who do not voluntarily comply. Their products remain a danger to their customers, society and the economy. Besides the fact when others do not deploy, chances are no one will, as there remains a smaller positive incentive to do so. In fact, it is negative as only money is lost when cheaper, non-compliant products win out on the market. Internet of Things security is a not a topic that end users should be concerned about, primarily. It is too much bother and for most too complex. When built in, there is no need to act as end user. Just like he does not have to act on security when buying a car or plugging his new refrigerator in the socket. Just to use it in a sensible way.

The European Commission held a consultation in the fall of 2019 on articles 3(3)(e) and (f) of the Radio Equipment Directive[104] requesting "*to contribute to the data collection exercise on the initiative relating to (i) the protection of personal data and privacy and (ii) the protection from fraud in*

[104] 2014/53/EU

internet-connected radio equipment and wearable radio equipment"[105]. The Dutch regulator of this Directive, Radiocommunications Agency (Agentschap Telecom or AT), already announced to regulate in the form of testing and active reach out to manufacturers of unsafe devices on the basis of the current Directive when IoT devices connecting to the internet through WiFi do not sufficiently protect end users' data and privacy. It has e.g. opened a complaint page on its website for end users to report[106]. In the meantime, the AT actively lobbies to change the Directive to containing baseline security requirements[107].

A way to raise awareness on this topic is to collect data on the costs on the one hand and the harm done through insecure devices on the other and share that data at the right levels.

Codes of conduct and discussions raise awareness, procurement creates a pressure point, rules set a standard. Regulation clearly is another pressure point in securing IoT devices.

Subset 4: Communication and internet standards

7.7. Awareness campaigns and raising awareness

7.7.1. Plausible deniability

Currently many companies in the internet industry can claim, and chances are truthfully, not to be aware of certain standards. Those who are not active in standard organisations, do not subscribe to or read mailing lists, etc., can plausibly deny being aware of security standards, let alone the need to deploy them. So how can be made sure that plausible deniability becomes obsolete? A few solutions already came by.

There are many and diverse awareness campaigns, but often aimed at end users, whether consumers or (small and medium sized) businesses. Concerning the deployment of internet standards in most cases there is no role for the end user. The technical community, as was already pointed out, often reaches out to (internet) technicians, who are not in an influential, decision-making position.

Responsibility for deployment lies solely with the service provider, platform, domain name holder or manufacturer. So, awareness campaigns should also be directed at them. This can happen in many ways. ECO, the internet industry association of Germany, indicated it contemplates a new action aimed at the deployment of DNSSEC in Germany in 2020. By creating clear cut narratives how abuse and harm could have been prevented by deployment, it hopes to create more awareness on the need to deploy[108]. If it were to reach out to other stakeholders outside its own industry, even more success could be possible.

[105] https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en (accessed 23-01-2020)
[106] https://www.agentschaptelecom.nl/documenten/formulieren/2019/09/25/melden-onveilige-slimme-apparatuur (accessed 23-01-2020)
[107] https://www.agentschaptelecom.nl/actueel/nieuws/2019/09/25/digitale-veiligheid-slimme-consumentenapparaten-niet-op-orde (accessed 23-01-2019)
[108] Shared in an interview

The IETF publishes its standards (process) online. After the publication of a new standard its work stops. Several participants in this process pointed out that communication on new standards could be bettered in several ways, in part a change of narrative. E.g.:

- The dissemination of the standards could be bettered by way of involving different channels of communication. E.g. by notifying relevant government departments and or agencies, industry and trade organisations;
- A “translation” of a new standard is called for, so that less technical persons understand the importance of the standard as well. This is not just important for non-technical people but also for people who have to deploy but are less highly educated;
- A management translation is of utmost importance as the manager / owner decides to allocate resources for said deployment.

7.7.2. Setting a common deadline-day

Another way is through incentivizing industry. On day xx the world moves into another standard collectively. The example often used is the IPv6 day that did not so much lead to mass adoption but certainly increased awareness. So, if all relevant players in the world could agree to such an initiative it becomes much more attractive to comply. Whether in creating more secure websites or in domain name validation, etc., an initiative would lead to pressure to comply. This is a topic that could easily be discussed within the IGF by bringing all relevant stakeholders together and discuss the way forward and overcome the inherent obstacles.

Creating awareness in combination with an action plan is another identified pressure point.

Raising awareness creates a higher pressure on organisations to deploy.

”Translations” make standards and their implications understandable at all levels.

7.8. Consumer organisations campaigns

Where internet security is concerned, consumer organizations have a role to play by comparing different services / products on the implementation of security (standards). By making it standard when scoring products also to take into account the ICT components, the security of devices would become better known to the consumer and the market as a whole. Are certain standards deployed, are the requirements of certification met, do manufacturers provide updates and for how long?, etc.

7.8.1. OWASP top 10

A good example is the following. The Dutch Consumentenbond (Consumer Association) had the 100 biggest webshops hacked on the basis of the OWASP top 10. The results proved quite telling and the pressure of this test was felt quite keenly by those involved, including the branch organisation[109]. Through a test like this, not only consumers are made aware of security options and are offered options to choose from, also industry feels a pressure and can see the comparisons for themselves. If more consumer organisations were to score by taking digital security into account, more consumers become aware of the options and will chose a product accordingly.

7.8.2. Privacy

Another example is the test Test Aankoop[110] (Test Buy), a Belgian consumer organisation, ran and published on in January 2020. It bought 14 food and health apps and tested them on respecting privacy[111]. Not surprisingly the results showed that the data the apps gathered were not secure. Except for one app, all shared privacy sensitive data with third parties, all but four did not live up to their privacy statement and two shared health data with third parties. Complaints were filed with the Belgian privacy commission.

Another example is the organisation NOYB who filed a complaint against Amazon on behalf of an Amazon seller on the basis of art. 32 GDPR[112]. Email traffic is send via Amazon without the internet standard TLS in place. Although TLS is not one of the examples used in this report, it is an example how on the one hand huge platforms tend to not use available internet standards securing their customers and on the other how societal pressure may change this.

The formal description of TLS or Transport Layer Security is: "*The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery*"[113] or in more laymen's language "*TLS is like an envelope around a letter. If not used, anyone can read the content of an email in transfer*"[114].

Whether a court case is the right way to force a platform towards deployment remains to be seen. It is a clear way to draw attention to insecure email and connections and another pressure point.

7.8.3. Future reach out

Active outreach to the European consumer organisations was foreseen as a part of this program but was financially not attainable. This is unfortunate as the interest from that side had already been expressed. A representative indicated that he fully understands the concept of what their role could be where the deployment of internet standards is concerned. E.g. through scoring (IoT) products or services in a different way by adding ICT related test components. This way consumers are made

[109] https://www.consumentenbond.nl/online-kopen/veiligheidslekken-bij-webwinkels.
[110] https://www.test-aankoop.be/action/over%20ons/onze%20geschiedenis (accessed 29-01-2020).
[111] https://www.test-aankoop.be/action/pers%20informatie/persberichten/2020/food-and-health-apps (accessed 29-01-2020).
[112] https://noyb.eu/complaint-amazon-doesnt-allow-baseline-tls-security/ (accessed 21-02-2020)
[113] RFC 5246 https://tools.ietf.org/html/rfc5246 (accessed, 21-02-2020)
[114] https://noyb.eu/complaint-amazon-doesnt-allow-baseline-tls-security/

more aware of internet security and manufacturers of the need for products to be secure by design or default. This is a potential pressure point coming from society at large that could lead to deployment. The desire it to take this up in 2020. It will be a part of a second iteration of this program. As this quote shows, cooperation could be most welcome:

> *"National Regulators and legislators need to be proactive and engage with industry stakeholders, standards Organisations and Consumer Groups to ensure that industry technocrats do not employ standards that are more tilted to single company policies. Important issues such as interoperability, standardisation, privacy, liability, dominance, transparency, intellectual property, data protection and security should be addressed in timely fashion as further delays could mean the disruption of the industry at the later stage…"*[115]

Scoring ICT / IoT products and services including standards and security measures is another identified way to apply pressure.

NGOs addressing non-deployment is another pressure point in society.

7.9. (Academic) studies

After the anti-botnet initiative Abuse Hub opened in The Netherlands in 2013, the Technical University of Delft was commissioned by the Dutch government to make an inventory of the results of having a botnet mitigation centre and whether the ISPs complied to being alerted to an infection on their respective networks. The study made it possible to score and show these results[116].

Often this is called 'naming and shaming'. That may not even be necessary. The way chosen in The Netherlands did not lead to shaming. There is a pressure on the industry simply because they are monitored actively, and no company wants to be the one lagging behind or show bad figures as an industry. Incentives are created to e.g. deploy security measures that drive the chance of infections of end users down. The other side is that a lack of improvement will entice governments to interfere when all else fails.

Studies by a neutral stakeholder apply pressure on industry and provide insightful knowledge to other stakeholders, another pressure point.

7.10. Naming, shaming or faming

Both previous examples point in the direction of naming and shaming. Some participants move beyond this. It is not necessarily the naming and shaming that is of relevance, awareness is only

[115] Connection and Protection in the Digital Age, Consumers International. https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

[116] E.g. Evaluating the Impact of AbuseHUB on Botnet Mitigation. Final Report. Michel van Eeten, Qasim Lone, Giovane Moura, Hadi Asghari, and Maciej Korczynski (Faculty of Technology, Policy, and Management Delft University of Technology, 2016)

created when the full impact of the results of flaws, behaviour and non-deployment become fully visible for all to see.

It is often said, that the world is waiting for the big bang in cyber security. In our opinion, the world has seen several in the past decade. Whether in ransomware crippling organisations, banks being digitally robbed, billions of privacy sensitive data lost and hacks into vital infrastructure, blacking out whole regions. For some reason, to date no incident seems to be big enough. So, is it necessary for a hack to cripple a whole country for months, with multiple deaths as a result, before truly serious action is taken? It is not to be hoped. Or is it because current incidents perhaps are too overwhelming already to respond to as a society right here and now? It is again hoped not to be so. So, what is a sensible next step?

Would this change when the source of the incident is attributed? Not (primarily) as in country A or Z or person B or Y, but by pointing out what flaw was used. The incident was successful because of …. This product did not contain …. It was one of the recommendations on ways forward. Collect data on the dangers and show the economic consequences to all concerned.

Another way of stimulating the use of best practices and standards deployment is faming. This has been outlined in more than one break-out session. The organisations behaving best could receive a quality mark, good press, etc. Checks can be made by independent bodies like consumer organisations, auditors, regulators, etc. See for example how Internet.nl ranks participants and lauds the best efforts[117].

Transparency about the sources and consequences of incidents is one and faming another pressure point.

7.11. Providing a new narrative

A new word entered the Dutch language in the weekend of 18-19 January 2020: "Citrix-traffic jam" (in Dutch "Citrix file"), meaning extra-long traffic jams due to a recommendation to shut down the Citrix application after the discovery of a bug in Citrix servers, causing people to travel to work instead of working at home.

It is time to make a clear divide. The deployment of internet standards itself is a technical issue, all surrounding it is not. The decision to deploy said standards is a decision made by managers or the board. It is a decision on how to allocate resources. This is an important distinction. Deploying standards is about offering security to an organisation itself and to customers, about offering a better product, about creating a competitive edge. As this is non-technical, the world has to find an alternative way the topic is discussed, a change of narrative, to take it out of the technical realm. To take it to the level where decisions are influenced and made. That comes with changing the language, tone and decision-making indicators, e.g. as written in a Forrester report:

[117] https://nl.internet.nl/halloffame/.

"In today's competitive marketplace, security has become a crucial market differentiator. Companies increasingly realize that security is critical to: earning customer trust; securing intellectual property; and protecting the brand"[118].

Companies working from this vantage point start to create their own positive business case by taking active measures at protecting themselves, their digital products and environment. Something that was pointed to by the Safe Software Alliance as well. Trust will become an ever-stronger incentive to do business and this includes, safe and more secure products.

7.11.1. Training CISOs

The above leads to a very specific recommendation. Chief Information Security Officers (CISO) usually are not part of the boards of companies, resulting in a dependency whether financial support is raised or not for cyber security within organisations. It is of importance for CISOs to convey their respective priorities, e.g. the deployment of internet standards, in the right language and style. If there are no training courses for this in your country, someone should start one. It could make a world of difference where taking measures resulting in higher levels of cyber security is concerned. Again, changing the narrative comes forward as important.

Communication (by CISOs) leads to better insights, questions, interactions and thus pressure points.

Making companies aware of the competitive edge they can create for themselves by being more secure than competitors is an important, economic pressure point.

More in general, eradicating plausible deniability is another pressure point.

There is an overall comment on communication of essence. Stakeholders have to reach out to others if the challenge of deployment is to be solved.

Subset 5: Implications for education curricula

7.12. Education

It is impossible for this report to even make a start on reporting on how educational curricula in ICT related courses, from vocational training to university, are compiled. Chances are that this may differ from country to country, most likely even school to school and university to university. What has been found out from the information received, is that curricula may be (extremely) outdated and that there is a shortage of ICT trained students leaving schools and universities in all parts of the world and at all levels. Participants shared that, at the moment, many of the course material computer scientists or website builders in vocational training are taught, does insufficiently take into account internet web architecture, internet security and security standards, or is outdated in general. It was stressed that it is often difficult to influence and change a curriculum to better suit the ICT

[118] Better Security And Business Outcomes With Security Performance Management Mitigating Risk And Generating Revenue With Metrics That Matter, Forrester September 2019, page 1

industry. Some who have actively tried to do so, indicated to have given up over the past two years[119].

In the break-out session of the workshop education was discussed. The discussion ranged from educating the public, which lies outside of the scope of this project, to courses. No true ways forward were formulated, if such a thing is possible in 45 minutes, but potential ideas for further discussion were identified. Including public – private cooperation, that also came forward in some of the interviews held.

The points that stand out show that education has a role to play. Internet safety and security must become something normal to teach at the earliest level. Educating the teachers is pivotal for this to be successful. At a later stage / higher level the Internet's architecture must be a part of the curriculum.

The solution lies in public - private partnerships where the private sector could start up initiatives to enrich the curricula of these internet-related studies with information directly from the field. Governments could (co-)fund the programs through subsidies. Also, these studies could focus more on the basic principles on which the internet and computers function rather than on specific coding languages. Training students can also take place after they have left their institute of education and are hired by companies. Programs training them on the job would be most efficient. This could also happen by bringing trainees together to save costs.

Large corporations like Amazon, Google and Microsoft initiated educational training programs, often re-schooling programs. However, they are mainly focused on increasing the amount of people wanting to be educated in computer sciences or programming, they can play an important part in spreading basic knowledge of digital hygiene and security in general, and on the latest internet standard for more advanced levels.

Many questions remain here that do not yet have conclusive answers. It may be worthwhile to bring together stakeholders from relevant communities and ask them to come up with recommendations for the world at large.

Subset 6: Stakeholder interaction

7.13. Communication from / to the IETF

Almost all stakeholders agreed that the policy making community and the technical community need to communicate better. Something underscored by the GCSC: "(…) *recommends establishing a standing multistakeholder engagement mechanism to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted*"[120]. Early interaction may prevent policy makers and parliamentarians from overreacting after serious incidents. To achieve this, the internet standards debate needs to be(come)

[119] As stated in interviews

[120] Advancing Cyberstability, page 27

comprehensible for people with a non-technical background. This comes with a host of layers and potential actions.

The relative isolation in which technical internet bodies work, causes them and its standards to be relatively unknown. The products they publish have too little effect and the traction the standards receive is far too low compared to the significance they stand for and ought to receive when discussing cyber hygiene. Looking at it from a positive angle, there is a world to win for the technical community and the standards they produce.

In general, people pointed to a few mismatches between stakeholders. Those who make the standards don't always take into consideration the operational challenges that come with implementing them. They also could become better at marketing the results of their work, driving deployment. Also, there is by far not enough communication between policy makers and the standard making community. Both of them need to understand each other better and learn about how to prevent harm in each other's functioning. The following comments came forward.

- Policymakers need to understand what the internet standardisation bodies, e.g. IETF, W3C, etc., achieve, where standards come from and what they stand for / aim to achieve.
- Internet standards making bodies could be more outreaching to other, non-technical communities.
- There is a clear need to understand each other's positions (better).
- The technical community is in need of understanding that standards can have an influence on government policies and have financial, economic, technical and educational consequences, for many others.
- "Translation of standards" for non-technical stakeholders is necessary to secure proliferation in a swifter manner. Many see a role for ISOC here.
- A test phase for new standards is called for.
- A time frame for deployment is desirable if not necessary.
- Where possible a positive business case should be built into protocols / standards.
- Policy makers should be able to flag issues to standard bodies and request solutions.
- Standard bodies could be more inclusive to those who cannot (afford to) travel to or participate in meetings but have valuable opinions or solutions.

To achieve this, technical standard organisations are advised to consider a form of consultation phase, where the standard to be is explained and stakeholders together can work out a strategy towards swifter deployment.

7.14. Potential ways forward outside of recommendations

Subset 1 to 6 translate into six recommendations presented in Chapter 8. There are other options that can drive deployment, yet are not caught in the recommendations. Some examples are presented here.

7.14.1. White hat hacking

Code is written by humans and they tend to make mistakes. Products are driven to market without proper testing so the time to market is shorter and profits made sooner. The Secure Software Alliance, IoTSA and others have made suggestions on how this could be bettered during the production process. Even if this way of producing software would be widely adopted, chances are mistakes, so vulnerabilities in the code remain in place, though less so.

One thing is certain. The people exploiting these vulnerabilities, either by using them themselves or to sell them as a zero-day exploit[121] to criminals or state actors, are testing software, websites and products 24/7 around the globe. They have a strong financial incentive to do so. The defending side does not. The longer a flaw is not found, the longer the necessary investment to create a patch is delayed. Actively finding flaws costs money and every flaw detected means having to come up with an action and / or a patch, driving up costs, earning nothing. Yet the world is in need of a safer internet and ICTs.

Marc Goodman, a former law officer, provided a possible solution for safer ICT services and products in his book 'Future Crimes'[122]. Governments and corporations could entice hackers to join a program to hack whatever they can, within the boundaries of responsible disclosure[123], and report vulnerabilities in designated places[124]. This could easily make 10.000s and most likely more, contributions to a more secure internet instantly available.

As an example, the city of The Hague invites hackers once a year to come and try to hack the city's systems[125]. Each time the city is a little safer. It is an example of how individual organisations can make themselves safer and thus their customers by proxy.

Working a program like Goodman suggests, creates multiple pressures on industry to perform better. Not only are flaws recognised in a timelier way, it will make security by design more attractive as it becomes cheaper to deliver a product that is tested in the production phase and thus more secure than having to patch and test continuously afterwards.

[121] "*A zero day exploit is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software)*". Wikipedia (accessed 2-1-2020)
[122] Future Crimes. Marc Goodman. Doubleday 2015, from page 373 onwards he provides many solutions for new ways of thinking about and looking at cyber security
[123] "Responsible disclosure is a vulnerability disclosure model in which a vulnerability or an issue is disclosed only after a period of time that allows for the vulnerability or issue to be patched or mended". Wikipedia (accessed 10-12-2019)
[124] One example of a disclosure that made the news recently is the U.S.' National Security Agency reporting a vulnerability to Microsoft, 14-01-2020
[125] https://www.denhaag.nl/nl/in-de-stad/nieuws/pers/ook-buitenlandse-hackers-bij-hack-the-hague.html (accessed 10-12-2019)

Stimulating white hat hacking is a way to turn up flaws in software, services and products and thus a strong pressure point.

7.14.2. Norms

The Best Practice Forum Cyber Security over the past two years has been working on identifying norms in cyber security. In 2018, the BPF Cybersecurity focused on the culture, norms and values in cybersecurity[126]. In 2019, this BPF continued its work by identifying best practices related to the implementation of the different elements (e.g. norms, principles, initiatives, frameworks, policy approaches) contained within a variety of international agreements and initiatives on cybersecurity[127].

The importance of this body of work comes through in some comments that have been received. “Norms should be developed”, one of the participants of this project stated. They are and already have as the BPF Cyber Security and the work of countless commissions and organisations attest to. The questions concerning adherence to the norms are the ones in need of answering. Voluntary norms remain voluntary, no matter how important these norms are. A next step for the BPF could be to identify how to translate identified norms into action, something the GCSC Norms Observatory currently strives to achieve and whether the breaking of norms can become attributable. Not only as to who perpetrated the norm but also who facilitated the perpetrations by non-deployment. The BPF has indicated attribution is to be a part of the 2020 program[128].

An example of how the breaking of norms can be attributed, was shown on Thursday 20 February 2020 when many countries attributed the attack on Georgian websites and TV stations on 28 October 2019 to the Russian Federation. As voiced by the Latvian government in its statement: “*Latvia joins the international community in condemning a massive cyber-attack against Georgia in 28 October 2019. The cyber-attack targeted Georgia’s government and private companies’ websites as well as the national TV stations. Latvia shares in the views expressed … which attribute the cyber-attack to the Main Division of the General Staff of the Armed Forces of the Russian Federation*”[129].

The attribution of norms breaking can be a pressure point towards deployment.

7.14.3. A radical solution: a new internet

A final group of participants advocated a radically different solution: create a new internet. Work on this solution is actually being carried out and published on. It is beyond the scope of this project to

[126] https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2018
[127] https://www.intgovforum.org/multilingual/filedepot_download/8395/1754 (accessed 27-12-2019)
[128] Draft program shared with the BPF, February 2020
[129] https://www.mfa.gov.lv/en/news/latest-news/65504-latvia-condemns-cyber-attack-against-georgia (accessed 21-02-2020)

integrate this topic in a wider fashion. For those interested start here[130]. If it is of interest to pursue within the IGF, it can do so in 2020.

7.15. What seems to have worked well

Participants have pointed us to several examples of best practices[131] that have, some, impact on deployment. They are mentioned here as examples for others to learn from.

7.15.1. Consumer power

The Dutch Consumentbond compared the top 100 webshops of The Netherlands on cyber security standards for websites[132]. They had them hacked by a penetration test company, Onvio, that tested on the recommendations of the OWASP top 10. The results were published by Consumentenbond. An action like this creates instant awareness. Not only with consumers but also with the companies involved and at the trade organisation representing the webshops. Undoubtedly many websites have been updated to comply with the OWASP top 10.

7.15.2. The Dutch Polder model

The Polder model is uniquely Dutch and perhaps hard to replicate in other countries due to different reasons. However, working through a neutral actor without its own agenda, is a way that stakeholders with conflicting backgrounds can try out cooperation, to find common ground and solve, in this case, internet security issues. A neutral organisation like ECP, platform for the information society, in The Netherlands is a model that is worthwhile to look into for all countries. As mentioned, the IGF could function as a neutral platform at the global level.

7.15.3. World IPv6 day

World IPv6 day is an example of how to actively create attention and impetus for an internet standard without a business case. It did not produce a massive global implementation of the standard but did attract a lot of attention. Several participants pointed out that this example can be used in the near future for certain, relevant and urgent security standards. An addition would be however, to involve other stakeholders than solely the technical community.

[130] 'Ambitions for Europe 2024'. Cerre White paper, September 2019, p 52-53.
[131] Responses to our survey near exclusively pointed to Dutch initiatives. We do not want to imply there are no examples elsewhere, just that no one pointed us to them. With one exception MANRS.
[132] https://www.consumentenbond.nl/online-kopen/veiligheidslekken-bij-webwinkels (accessed 4-12-2019)

7.15.4. Actions on standards

Some organisations actively propagate the deployment of a certain standard. Giving the topic more and wider attention as well as importance. Examples like Deploy 360 and MANRS have been provided. The past proved not to be overly successful. This led to the conclusion that new and different actors should be getting involved and narratives changed. New approaches in reaching out to and involving others than the usual suspects can be experimented with.

7.15.5. Internet.nl

Internet.nl is a website that slowly but surely entices organisations and corporations to clean up their digital act. On the website a website / domain name, the email address and the connection used can be tested against a certain amount of open internet standards. The score says something about the level of security and explains what next steps are. The project started with just three standards tested and is slowly growing. In fact, three more standards were added during this writing process and RPKI is considered as the next option. There is a hall of fame showing those who score well.

Internet.nl is an "*initiative of the internet community and the Dutch government*" [133] and open source. The source code behind Internet.nl is available to anyone wishing to adopt the program in his or her respective country.

The European Commission has a more elementary email security checker online called 'My Email Communications Security Assessment or MECSA[134].

7.15.6. Pas-Toe-of-Leg-Uit (Apply-or-Explain)

Another initiative led by Standardisation Forum in The Netherlands is a list of open standards any organisation ought to have deployed. For governments buying ICT products these, currently 42 standards, are mandatory to ask for. This list is actively distributed and can be used as an indication for industry to at a minimum copy. Any government organisation not applying these standards is subject to the demand to explain why it does not[135].

It needs reminding that all these efforts are voluntary to use and there are no, real, consequences attached to non-deployment. The question remains whether these efforts are enough to reach mass deployment, despite the steady rise of deployment over the years[136].

[133] https://www.internet.nl/
[134] https://mecsa.jrc.ec.europa.eu/ (accessed 02-02-2020)
[135] https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht (accessed 10-12-2019)
[136] Meting Informatieveiligheidstandaarden september 2019. Forum Standaardisatie

7.16. Deployment in limbo

Having accumulated the data over the past months allows to gain a level of knowledge that is not easily available. It makes it possible to connect dots and arrive at new insights. In the survey and most interviews, the main reason provided for the slow pace of deployment provided was the lack of a business case. This is perhaps more a result than a reason.

Everything surrounding the deployment of internet standards points to a collective action problem. Next to that internet standards play a very small role, if any, in formal texts and laws. Combine this with a far from ideal level of communication between important stakeholders and an explanation is found why internet standards are relatively unknown in places that matter, let alone that many people of influence understand what role these standards could play in securing the internet and all its users. They never even enter the debate because of their (lack of an) information position. Yes, there is no business case, but that is only because a situation exists in which very little people, in a formal and often informal sense, seem to care whether a standard is implemented or not. There is no carrot and certainly no stick, anywhere. Some nudging at best. It is an easy topic to ignore for all who want to. A sluggish deployment is the practical outcome of the status quo.

This points to a situation that lies beyond the lack of a business case. Internet standards seem to hang in a kind of limbo. Having the importance of the protection of the public core of the internet in mind, the question several stakeholders need to answer for themselves is, is this the position you want to be in?

Both angles need further work to establish root causes. At this point there is no time left for further research. For now, it is just an interesting, striking observation.

8. Recommendations and the way forward

A comment from a dignitary presenting at the IGF struck a note. He said that we tend not to look at the cost of implementing security but at the cost of losses and mitigation, i.e. after the incident. Just think of the decision at Maersk to save a few million euros by delaying the install of a Microsoft update, a fact to be found only hidden deep within publications, versus the broadly shared headlines on the huge loss due to the ransomware cum sabotage infection that was successful because Windows had not been updated. And what to think of Boeing? Was the software in the Max 737 not tested in an agile way during the development phase? Or was it the board deciding that it was time to market?

In this report the results of this body of work were presented. This leads to six recommendations, action plans. This chapter finally presents suggestions for the continuation of this pilot project.

8.1. Recommendations

1. ‘*Create a business case for the deployment of internet standards*’.
2. ‘*To deploy internet standards successfully they need to be incorporated by reference into law or legally binding regulations, including a designated regulator*.’
3. ‘*To deploy internet standards successfully requires building security by design / default into products and services*’.
4. ‘*All stakeholders should collaborate on coherent strategies for multilingual awareness raising on internet standards and their effect on internet security’.*
5. ‘*Internet standards and architecture must become part of education curricula*.’
6. ‘*Standardisation processes are advised to include a consultation phase with government and industry policy makers, and civil society experts*.’

Recommendations are nice to have, but without an action plan where key players commit to, they remain nice to have. Hence, they were tested in the workshop and the interviews and joined to potential next steps. This made it possible to identify pressure points[137] in society and the formulation of potential actions and ways forward, including the necessary stakeholders. So, what next steps towards deployment can be identified?

[137] In annex 3 an overview of all identified pressure points is presented for your convenience

8.2. Proposed actions

It is a safe conclusion to state that no one participating in this project desires legislation decreeing the deployment of internet standards. To subscribe to this conclusion, however, comes with a moral obligation if the true goal is to be reached: the swifter deployment of internet standards making the internet and all its users safer immediately after mass deployment. The moral obligation is to recognise the necessity to look at and work on alternative next steps. They are presented here.

8.2.1. Action 1. Self-regulation vs legislation

The question is important, as two things have been established, yet not satisfactorily answered. Although undesirable, many participants see legislation as the only way forward if deployment is to become the norm. And, legislation is the easiest, quickest and most likely cheapest way to ensure a level playing field and deployment. There are many arguments against legislation and regulation and they all should be assessed. Only then is a true answer on this way forward possible.

Working group 1 law: governments/policy makers, parliamentarians (IPU?), technical community, industry, consumer organisations/civil society

Task: Answer (and add to) the questions posed earlier on this topic and make an inventory of and assess arguments in favour and against legislation. Decide to legislate or not and if so what kind of legislation. And, determine whether there is an alternative to legislation and what actions from whom are necessary to deploy successfully.

Working group 2 regulation: governments/policy makers, regulators, technical community, industry.

Task: Determine in how far current laws allow for regulation on deployment of internet standards, debate certification or quality controls.

8.2.2. Action 2. Dissemination of internet standards

There is a need for more interaction. Through consultation new standards can be explained, dissemination strategies discussed and the knowledge on why to deploy the internet standards spread. This leads to a few different tasks to work at.

Working group 1 interaction: policy makers, technical community, industry, ISOC, civil society

Task: Work out how information can be exchanged, knowledge gained both ways and relevance to policy determined.

Working group 2 Dissemination: policy makers, technical community, ISOC, trade organisations, industry, civil society

Task: Determine how to “translate” standards for the world to understand and how a new standard is disseminated to all involved, provide the narrative for CEOs, CFOs and boards.

Working group 3 training programs: policy makers, technical community, industry, trade organisations, education representatives

Task: Train the trainers who are to assist deploying standards within companies.

8.2.3. Action 3. Platforms

Many individuals, SMEs and organisations make use of platforms for ICT and internet services. These platforms decide themselves what level of security they offer, usually without the “user”, or in old-fashioned terms “customer”, having any influence on the level of security. This means that one of the quickest wins would be if these platforms step up their game. Governments together with consumer organisations, trade organisations and large corporations could apply pressure on these platforms to make their internet / ICT services more secure.

Working group: policy makers, governments, large corporations, trade organisations, consumer organisations, civil society and internet / platform industry

Task: Describing minimum levels of cyber security, discuss certification, deployment phase, pricing

8.2.4. Action 4. Internet resource organisations

How to assist internet resource organisations to effectively combat internet abuse and co-defend the public core of the internet?

Working group: Internet resource organisations, policy makers, law enforcement, industry

Task: define abuse, (the making of) existing and desired policy, cooperation and suggest ways forward

8.2.5. Action 5. Create a positive business case

Can a positive business case for deployment be developed and what conditions need to be met?

Working group members: representatives from governments, large corporations, trade organisations and internet industry.

Task: Describe a positive business case, how to raise demand, create a minimum overview of necessary standards, pricing.

8.2.6. Action 6. Education programs

For the internet to become more secure, knowledge on how to make it secure needs to be readily available. Educational programs in schools and universities have to make internet security a part of their respective curricula. Per country it has to become clear who is responsible for education programs and for training teachers. Through cooperating with industry, governments need to alter curricula at all levels, starting at a minimum in high schools, preferably in primary school. Training programs for employees already on the job and retraining programs could be created through a common effort of industry and government.

Working group: policy makers, representatives of schools and universities, industry, technical community

Task: Define education programs, define topics, define roll out, funding and participation

This action is in EuroDIG's 2020 program. The results will be fed into IGF processes.

8.2.7. Action 7. Internet of Things / safe software standards

Despite some activities having been identified around IoT, the question was raised whether these are enough. If regulation or certification becomes a norm, ideally the standards are of a global nature. This involves harmonisation of measures and certification.

Working group: policy makers, technical community, industry, manufacturers

Task: Define IoT categories, define baseline security for IoT categories, certification, discuss deployment phase, legislation, regulation, pricing. The same goes for software.

The IoT topic is worked on extensively in many parts of the world. At the same time it is extremely urgent. There may be a use for an international secretariat where developments can be monitored, discussed, aiding global harmonisation where necessary / possible.

8.2.8. Good intention 1.

It is recommended to change the word "user" to "customer". It gives a fresh perspective to the relationships between customer and manufacturer as this seems to have gone lost in ICT. A user is usually associated with a dependence on illegal substances. Like the proverb says: "The customer is king". This frame of mind will aid a change of thought for all concerned.

8.3. Continuity within the IGF

There is one question that remains to be addressed and answered. This report does not solve the complex internet governance issue of internet standards deployment. It provides answers and potential solutions. It also identified the IGF as the neutral platform where all stakeholders can meet and participate as equals. The following proposal is put to the MAG.

Recommended is the continuation as a policy track. To make the internet a safer place is one of the great challenges mankind faces. The need for it is seen and felt every day. By making internet standards deployment a policy track, the MAG underscores not only the importance it gives to this complex internet governance challenge but also expresses its ambition in showing the world how the IGF can assist in providing the world with potential solutions to deploy standards.

There are two principle reasons for this recommendation. The first is the need to build working groups; that currently do not exist. This is expected to be easier in a more formal IGF track. However, it is not about this decision itself, it is about identifying and approaching the right organisations. It is about asking them to commit people and resources to the process, to work on trust and cooperation, so they, together, can decide on the way forward. It is about taking ownership and feel responsibility for (the deployment of) the outcomes. The second is the content. Several working group topics are suggested, based on the recommendations. They have been presented in the above. Only after such a process, the first future results, the tangible IGF outcomes, can be presented in and soon after the 2020 IGF in Katowice. At that point in time it is clear which policy recommendations have to be taken up elsewhere, outside of the IGF or need to continue in some form within it. Finally, there is an active role for the IGF and the MAG to play.

8.4. The role of the IGF and the MAG

This report has identified a host of potential ways forward and pressure points in society to work at. Like all recommendations, plans of action and good intentions, they will only work if and when people and organisations commit to a common goal. Experience learns that after people from a different background have discussed among each other new ways to collaborate and find workable solutions, it becomes normal to discuss the route towards (potential) outcomes together. It is here that the IGF can play an important role. It is neutral, does not have its own agenda and can facilitate and support a process from this neutral position. As such it can facilitate so called intersessional working groups on particular selected topics during the year. The groups can present the outcomes at the IGF with a set of recommendations to be taken out of the IGF, to organisations where they are welcome and accepted as a common ground for further work.

The MAG chair and the members will have to play a pivotal role in bringing about the participation in the working groups. By reaching out, through active leadership and participation and by assisting in building the trust both between the participants and in the IGF itself.

8.5. Request for a MAG decision on a policy track

The MAG is asked to agree with a second iteration of the project in the form of a policy program. Although the first steps have been set, the most delicate step still needs to be taken: bringing all the stakeholders together and to create an environment of trust. This may take an active role from certain MAG members and most likely the chair. Once gathered, the policy track can be filled with topics mentioned in the actions above, working towards (tangible) outcomes. The request will be put to the MAG in a separate document.

This report presents the work of a few months. Both the work and the topic have been taken seriously. Imagine what the IGF is capable of achieving in the future. It would be a missed opportunity to stop the work this pilot provided now without finding out what it could truly and practically deliver. This is not the end, only the beginning.

Part 3. Epilogue

This report is the outcome of a pilot conducted within the IGF structure. Working within this structure makes it possible to share some lessons learned. There are also a few comments in general on internet standards deployment which do not fit in the continuity of the report but are worthwhile sharing.

9. Working within the IGF structure

Now that the pilot has delivered its tangible outcome in the form of this report, it is possible to write a few short words concerning the position of a pilot like this within the IGF and some lessons learned that the MAG may want to take into account in future (pilot) projects.

9.1. Project standing and continuity

Any future project needs a dedicated MAG member as contact person for the project team. It was not considered at the time of inception, but is important to have in future projects like these as information has to be exchanged that informs both sides. As a result, this project hangs in some kind of vacuum while it should have been rooted in the IGF. This is in line with the fact that at present no one owns the results of the project or expresses responsibility for its outcomes. To have a true impact this has to change and is one of the criteria for future decisions on projects. These projects need to be fully owned by the MAG as well as a certain responsibility accepted for the outcomes, to make sure they are disseminated and taken up elsewhere.

9.2. The IGF workshop on internet standards deployment

The workshop at the 2019 Berlin IGF led to a host of new insights from participants who shared their views on the deployment of internet standards from their respective backgrounds. It not only proved how hard it was to contain the discussion to the designated recommendation, but also showed the need for communication between stakeholder communities and the way they can aid each other. Many were of the opinion that silos need to open up if internet standards are to be deployed. This recommendation was welcomed as the sixth one, as this did not come out of the survey. It shows the added value of the IGF as a conference when it actively uses the experience and knowledge of those present.

To “solve” a complex issue in a one-and-a-half-hour session is an impossibility. It proved impossible to make the headway hoped for, despite gaining great insights. In future it is suggested to experiment with forms. What could have worked here e.g. is to spread input and output over the week. Participants meeting at regular points in the program, allowing for ideas to develop and be worked out further, leading up to a presentation on day 4 and a report after the IGF.

9.3. IGF Repository

One of the tangible outcomes of this pilot project is a repository of accumulated knowledge on the IGF website. There are many initiatives around the world, all with its own set of ideas and recommendations. As Fabrizio Hochschild, U.N. assistant secretary general, mentioned in Berlin, perhaps all studies should be collected and studied all to find the coherence. One of the goals of this project is to identify as many initiatives as possible from around the globe. What has been found was put into a repository on the IGF website. This has a clear goal. All those starting this process later on in time, can learn from the work that already has been carried out and distil best practices to copy. It creates a space where initiatives, whether policy, roadmaps, industry documents, etc., can be gathered. Something that can organically grow long after this project has stopped. The IGF website has a designated spot for it as part of this project[138].

9.4. The pilot project in the context of the IGF

The fact that this project was externally funded, that many individuals from different stakeholder groups from around the globe participated and shared their time, knowledge and ideas attests to the fact that the chosen topic and the IGF have been taken seriously. The presented outcomes give opportunity to continue within and outside of the IGF and provide solutions towards deploying internet standards that on mass deployment make all users instantly more safe when using the internet. The assumption that the IGF is a neutral platform allowing all stakeholders to join in an equal position also proved correct. It is what makes the IGF a unique global multistakeholder platform to address a complex issue like the deployment of internet standards is. Long-running internet governance issues are sometimes complex because interests are conflicting and / or because different stakeholders are not able to agree on a solution. It may hold true that trust needs to be built in order to set next steps towards cooperation. As a neutral platform, the IGF could work on an environment of trust and next steps, attracting all relevant stakeholders to come to the table.

9.5. The IGF+ model

If the IGF wants to have a true impact, like e.g. suggested in the “IGF+ model[139]” as a “policy incubator[140]”, projects under this model must be firmly rooted in the IGF structure. This should be one of the criteria for future decisions on projects. These projects need to be fully owned by the MAG as well as a certain responsibility accepted for the outcomes, to make sure they are disseminated and taken up elsewhere. Like it says in the U.N. report: “*Enhancing digital cooperation will require both reinvigorating existing multilateral partnerships and potentially the creation of new mechanisms that involve stakeholders from business, academia, civil society and technical*

[138] https://www.intgovforum.org/multilingual/content/implementing-internet-standards-and-protocols-for-a-safer-internet

[139] See e.g. ‘Considerations on High-Level Panel's "Internet Governance Forum Plus" Model’, William J. Drake. CircleId, 4 November 2019.

[140] The age of digital interdependence. Report of the UN Secretary-General’s High-level Panel on Digital Cooperation

organisations. We should approach questions of governance based on their specific circumstances and choosing among all available tools"[141].

If anything, this pilot project showed the IGF can achieve more than it currently does. The MAG has the opportunity to decide on what the IGF is to become. Not to do so will mean others will do so for the MAG and the IGF.

9.6. Active reach out to enlarge participation

Part of this project involved the active reach out to parliamentarians. Together with the combined efforts under the aegis of the German host, BMWi, this proved extremely successful. A part of the success is found in the dedicated program for this special stakeholder group. More, now absent, stakeholder communities need to find their way to the IGF. This can only happen through a) a dedicated reach out program and b) by reserving and organising a small part of the program filled with internet governance issues that are of relevance to that community. As they are absent and most likely unknown with the IGF cycle and process, there will never be a workshop request from these stakeholders unless it is offered to them.

9.7. Commitment and available time

What proved hard, was to get people committed before the IGF. Being in a regular environment makes it hard for many to commit time to a project that is extra to all else. This may change if and when the IGF becomes more output driven as a rule. What is important to recognise here, is that the people present at the IGF are usually not the persons needed for a project like this one. This leads to an extra step in ensuring involvement and commitment. At present, it shows that the most needs to be made of the IGF week itself. People decide to commit there and then.

9.8. Funding

Concerning the funding. With the exception of the reach out to parliamentarians, the project was funded by Dutch organisations. In the future this is not sustainable as this is a global issue concerning many and varied stakeholders. The MAG may want to think about a sustainable solution to fund an IGF intersessional project like this. Currently it depends on the activities of the project team itself and one-on-one funding of the team, which maybe is too uncertain, unknown or even impossible for non-Dutch organisations to fund. Ideally in future projects some kind of neutral fund should be involved, as e.g. IGF Trust Fund.

[141] Idem

10. Connecting the dots

It is important to first show that the participants in this project, knowingly and unknowingly depending on the level on which they participated[142], arrive at (a rough) consensus on several topics. First, the internet needs to become safer. Second, internet standards, if only deployed, contribute to a safer internet. Third, at least in most cases, a business case is lacking to deploy said standards. Fourth, legislation, though perhaps successful as a driver, is not seen as the answer and should be, at best, the last resort. Fifth, several participants both knowledgeable in the IETF standardisation process and the less so, stated: communication about the agreed upon standards needs to be bettered. Sixth, this is a collective action problem.

This leads to the conclusion that the recommendations hold up and need further work. They also are in part contradictory as (almost) no one is in favour of regulation / legislation, but many see it as the only solution. If no legislation is the preferred choice and deployment a prerequisite for a more secure and safer internet, decisive action in all other segments is called for, but remains voluntary. Self-regulation in that case becomes leading.

As there is a distinctive first mover disadvantage, self-regulation at this point in time has the odds stacked against it. This comes forward in the following examples as well. What are all stakeholders up against?

10.1. Comparisons and paradoxes

As a collective action problem internet standards deployment in general is comparable to environment issues. Also, here a first mover advantage is totally missing. It also is comparable to vaccine programs. They are only successful as a whole when inoculation remains above 95%. The same may be true for cyber security issues. When >95% participates, the security and enforcement world will probably be able to cope with the remaining <5%. Reaching that 95% is a gigantic task. One the world has not come close to solving yet. Who has to take the lead? Who has to follow, how, when, where?

In the results of our efforts several paradoxes came forward, which are important to grasp as they assist in explaining why deployment has a slow uptake.

10.1.1. Paradox 1

Without a doubt this is the most interesting paradox: nearly everyone tells us that there should be no legislation, yet a significant proportion of people answering the question what their recommendation is on how to solve this topic, points to the government and legislation / regulation as the only solution. So, if there is not to be legislation, then there can only be self-regulation from the industry or is there? This report presented several options, indicated possible direction and solutions. When

[142] On the basis of the survey results and the workshop

all is said and done though, it will take a collective action to create an acceptable level of safety and security. If this does not happen voluntarily only two options remain open to policy makers and parliamentarians: 1) Legislation / regulation or; 2) To give up and surrender the internet to those with nefarious motivations.

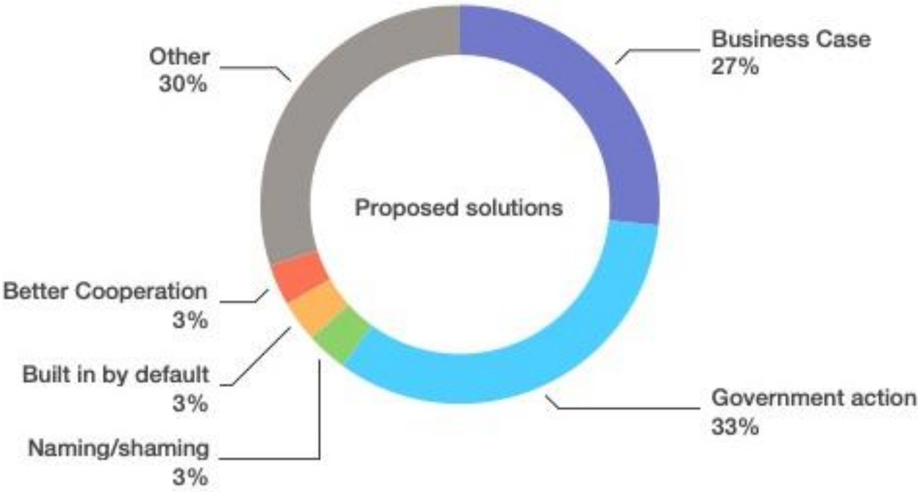


Figure 2. Survey data: What is your recommendation to the world at large to start deploying security-related internet standards faster than they are today?

10.1.2. Paradox 2

In 2019 most organisations (and individuals) are used to pay for defensive measures of all sorts, from anti-virus products to detection systems, etc., only making themselves somewhat safer. The willingness to pay for defensive measures that make the world as a whole safer is far less normal. E.g. building secure products by design, to secure websites, measures at hosting companies and platforms securing information, etc. Paying for that sort of security is what has to become the standard, for the individual and the common good.

It is the former part of defence that is most actively promoted by governments and e.g. banks through national campaigns. Anti-phishing campaigns, awareness campaigns, anti-botnet centres, etc. Campaigns that focus solely on the individual end user and mitigates the effects of abuse, instead of eradicating the source. Sources for abuse, where by far the most end users have no option nor (purchasing) power to inflict change. This question needs answering: What makes that government efforts in cyber security aim for the end users and not (also) the service providers and manufacturers? Despite what is at stake: national security in many guises and sizes. So how come governments depend, almost solely on the least competent of all where cyber security is concerned to take action: the end user? In order to proceed, this question begs an answer. One that is currently not at hand.

10.1.3. Paradox 3

Many governments propagate the protection of the public core of the internet but need to do more to assist in guarding the internet standards and bodies that are a part of the public core.

10.1.4. Paradox 4

Although the costs of cyber-attacks and incidents seem to increase steadily, incentivizing spending resources to make incidents and attacks less likely is not widely turned to as a solution.

10.1.5. Paradox 5

IETF members put in their best efforts into making the internet a safer place by making better standards. ISOC runs programs to make standards better known and understood within its community. Both organisations appear less willing to reach out to other stakeholders and work together towards deployment.

10.2. Common interests

"… Shows how, in our leaders' focus on maintaining digital weapons to attack our enemies, they've left our own critical infrastructure defenceless"[143].

If deployment is looked at from a meta level, it would seem that all nations, organisations and individuals, at least in theory, have the same concerns and a common goal. Each and every one does not want to lose valuable data, secrets, privacy, future policy, finances, etc., etc. All concerned do not want to be hacked, phished, infected, ransomed. This outset makes defensive measures of interest and worthwhile for all. So all, again in theory, should have a common goal to make the internet and ICT more secure. Insecurity potentially leads to enormous losses, collectively and individually. Seen from this angle, it ought to be a no brainer to use all measures that exist to make the internet and ICT more secure and all users safe.

Alas, from here it becomes more complex and the world currently is where it is at. No one involved contests the need for change, yet still has difficulty in speeding up the rate of deployment. If the true goal is to create a more secure internet and ICT environment, the paragraph right above this one ought to be the starting point for every single entity involved.

[143] Cory Doctorow on the backcover of 'Sandworm. A New era of cyberwar and the hunt for the Kremlin's most dangerous hackers'. Andy Greenberg, 2019

10.3. Dissemination

In order to make a difference this report will be disseminated broadly, including organisations that have not been reached (in full) yet. Another round of active outreach is foreseen, involving parliamentarians, policy makers, consumer agencies and the technical community. This way they all will learn about the causes for slow implementation and the potential remedies. A part of a second phase will focus on the facilitation of cooperation.

10.4. Final words

The executive summary ended with a comment to look at internet security in general with a different perspective. The internet, including devices and software, has become an integral part of our lives. A lot of it for the better. The other side is that the functioning of our societies fully depend upon a functioning internet and ICT. Ignoring insecurity starts to equal potential devastation. Too many examples of mass disruption already exist and need to be(come) understood for what they truly are. Especially by those in leadership positions. The question this report opened with, 'So, why are internet standards so slowly deployed?', has been answered.

Since we started writing the report the Covid-19 virus started spreading around the world. Daily updates are provided on how governments and health services try to contain the virus. This is the example of how internet security ought to be addressed as well. The stability and security of societies, no matter where you live, is at stake. A balance needs to be found between where individual decisions to invest in deployment of standards end and collective action becomes necessary if not mandatory. In health and in many other products this is a fully normal form of standardisation. For the internet and ICT it is not. It is time to take a broader look at the issue at hand and decide on how to proceed.

To make the internet safer takes efforts to bring all the different stakeholders and their controversies and different interests together. It may even take decisions no one can imagine making today. Not taking action is no longer an option, unless we all, governments, industry, organisations and end users alike, prefer handing over the internet to those with nefarious intentions for good. Shall we do our utmost to not let it come to that?

Annex 1. Support: A thank you

This project would not have been possible without the financial support of the following organisations.

- Federal Ministry of Economic Affairs and Energy (Germany)
- Ministry of Economic Affairs and Climate Policy (NL)
- SURFnet
- SIDN
- ECP: platform for the information society
- DINL

Many people and organisations assisted with the dissemination of the survey; assisted in making presentations to Members of Parliament possible or; provided advice and introductions. A final thank you goes out to all who participated by taking the time to fill in the survey, participated in the workshop or allowed us to interview them. Without you all this project would not have been possible. Thank you for your support.

The following organisations and persons assisted by other means

- African ICT Foundation
- Anastasiia Fito (Behance Profile)
- APNIC
- Arda Gerkens
- Ben Wallace
- Carsten Schiefner
- European Internet Forum, Maria Rosa Gibellini
- IGF secretariat, Anja Gengo and Luis Bobo
- Inter-Parliamentary Union secretariat, Andy Richardson
- Lousewies van der Laan
- Lynn St. Amour
- M3AAWG
- Mark Carvell
- Medienstadt Leipzig
- MELANI
- NLNet Labs
- Office of the late Jimmy Schulz: Jessica Langer, Verena Coscia, Juliane Hüttl
- RIPE Anti-Abuse Working Group
- Sandra Hoferichter
- Vereniging van Registrars

Annex 2. List of interviewed[144]

Andrea Lattanner, Microsoft

Andrew Campling, 419 Consulting

Arnold van Rhijn, Ministry of Economic Affairs and Climate Policy (NL)

Bart Knubben, Dutch Standaardisation Forum

Basil Ajith, sflc.in

Chris Buckridge, RIPE NCC

Danny Onwezen, Safe Software Alliance

Greg Bianchi, Microsoft

Karen Melchior, MEP

Gerben Klein Baltink, Internet.nl

Lars Steffen, eco e.V.

Marianne Azer, Egyptian MP

Marina Kaljurand, MEP, former chair GCSC

Michel Rademaker, HCSS

Michiel Steltman, Stichting DINL

Michele Neylon, Blacknight

Olaf Kolkman, Internet Society/GCSC

Pablo Hinojosa, APNIC

Paul Verhagen, HCSS

Peter Koch, DENIC

Raul Echeberria, LACNIC

Sebastien Bachollet, ICANN at large

Simon Hicks, Department for Digital, Culture, Media and Sport (UK)

[144] Some were asked only a few relevant questions, others were interviewed extensively

Annex 3. Explanation of standards

1. DNSSEC (Domain Name System Security Extensions)

Explained at the most basic level, the Domain Name System allows people to search for a domain name instead of via IP addresses which are much harder to remember. E.g. someone typing in ICANN.org will go to that organisation's website after the domain name (ICANN.org) is translated in the DNS system into an IP address (192.0.43.7 and 2001:500:88:200::7) designated to ICANN[145].

The DNS system was designed in the 1980s without security in mind. With the growth of the internet the fact that it was possible to redirect queries of end users to malicious websites, followed by consequent abuse, became a cause of grave concern. This led to the development of DNSSEC within the IETF[146]. Once deployed DNSSEC allows for the authentication and integrity protection of the data sent by the end user device and the DNS[147]. In lay terms, DNSSEC prevents someone to pose as someone else that allows connections to be set up with false websites usually with malicious intent or "spoofing".

2. RPKI (Resource Public Key Infrastructure)

"RPKI is a specialized public key infrastructure (PKI) framework designed to secure the Internet's routing infrastructure. It allows the members of regional Internet registries, known as local Internet registries (LIRs), to obtain a resource certificate listing the Internet number resources they hold. This offers them validatable proof of holdership (…). Using the resource certificate, LIRs can create cryptographic attestations about the route announcements they authorise to be made with the prefixes they hold"[148].

In lay terms, this makes it much harder to pretend to be someone else where the routing of internet traffic is concerned, leading to misdirected traffic usually for malicious intent.

3. BCP38 (Best Current Practice 38)

This IETF protocol is about Network Ingress Filtering to defeat Denial of Service Attacks which employ IP Source Address Spoofing. It prohibits "*an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules*"[149].

[145] https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en (accessed 3-12-2019)
[146] IETF started work on DNSSEC in 1997: https://datatracker.ietf.org/wg/dnssec/documents/
[147] https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en (accessed 3-12-2019)
[148] https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure (accessed 3-12-2019)
[149] https://tools.ietf.org/html/bcp38 (accessed 3-12-2019)

Or in lay terms, users using fake addresses are filtered out of the traffic coming into networks. This also prevents one of the causes of DDoS attacks.

4. OWASP top 10 (or 25)

The OWASP top 10 addresses the currently most critical web application security risks. It "*is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code*"[150].

In lay terms. If these rules are applied when building websites, they become instantly more secure as the low hanging fruit, and more, for hackers is taken away. E.g. placing malicious content on a website posing as an add becomes impossible, just like changing or adding texts.

5. ISO/IEC 27001 (International Organization for Standardization/International Electrotechnical Commission 27001)

ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. It requires that management:

- *Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;*
- *Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and*
- *Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis*[151].

6. Safe Software

Search the internet for safe or secure coding and many websites present themselves. This has not been pursued further, but not before the text that really stood out is presented here: "*Security is a constant battle*", pointing to the website of The Open Web Applications Security Project[152]. For this report a Dutch initiative was studied, in the knowledge that there is much more available in the world.

[150] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (accessed 3-12-2019)
[151] https://en.wikipedia.org/wiki/ISO/IEC_27001 (accessed 4-12-2019)
[152] https://contentlab.io/security-is-a-constant-battle-be-the-secure-code-warrior-in-your-organisation/

In the Netherlands, the Secure Software Alliance develops and actively promotes ways forward to assure application security by design. By incorporating security into the production process of soft and hardware, flaws are detected and mitigated before going to market. Following a process like this assures far safer products and security by design[153].

In the United States the IoT Safety & Trust Design Architecture and Risk Toolkit (ISTA) was published in April 2018. "*The goal of the ISTA is to help the market deliver on the promise of Internet of Things (IoT) by enhancing device security, safety and privacy practices*"[154]. ISTA has seven tenets as its guide, built from 45 principles.

[153] https://securesoftwarealliance.org/ (accessed 4-12-2019). The page also shows a link to the book the alliance published: 'Agile Secure Software Lifecycle Management'.
[154] https://agelight.com/istarelease.html

Annex 4. An overview of the pressure points in society

1. Create a financial stimulus
2. Organise awareness campaigns on the benefits of internet security standards
3. Enforce internet standards deployment through legislation and / or regulation
4. Have legislation / regulation as ready as the default option
5. Active questioning of relevant stakeholders by policy makers, politicians, consumer organisations, etc.
6. Include standards deployment in government procurements requirements
7. Codes of conduct / standardisation for websites, software, IoT devices
8. Include deployment incentives in the design process of internet standard
9. Use Internet of Things as a source for regulation or awareness campaigns
10. Organise awareness campaigns aimed at industry at large
11. Organise consumer organisation campaigns
12. NGO campaigns against lacking standards
13. Conduct academic studies on the topic
14. Transparency around sources and (financial) consequences of incidents
15. Use naming, shaming or faming
16. Awareness concerning the competitive edges provided by secure products
17. Eradicate plausible deniability
18. Provide a new narrative for non-technical stakeholders
19. Organise attention for digital security and standards in education curricula
20. Improve communication with the IETF
21. Encourage white hat hacking (events)
22. Train CISOs on the topic of communication with board level
23. Create norms on the deployment of standards
24. Attribute the breaking of said norms
25. Create a new internet

Annex 5. Background of the survey respondents

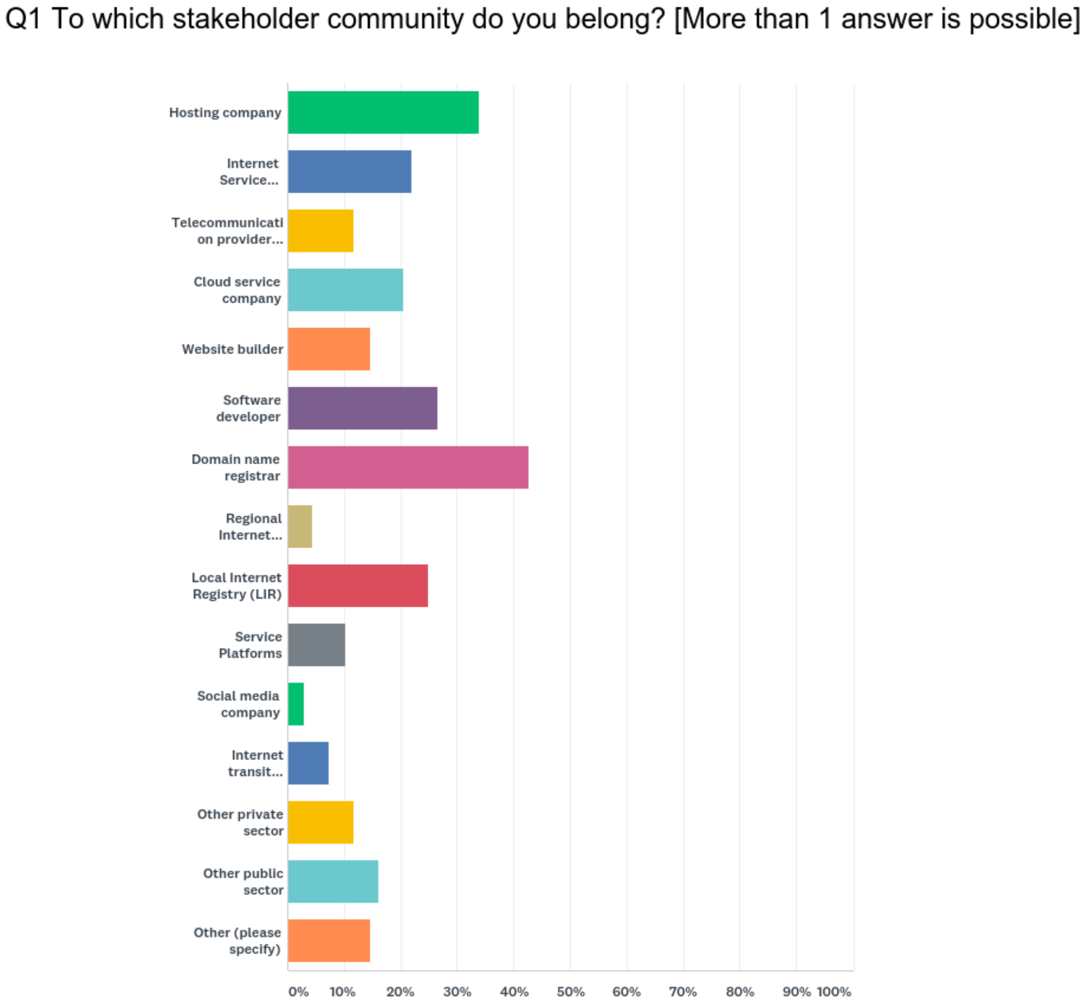
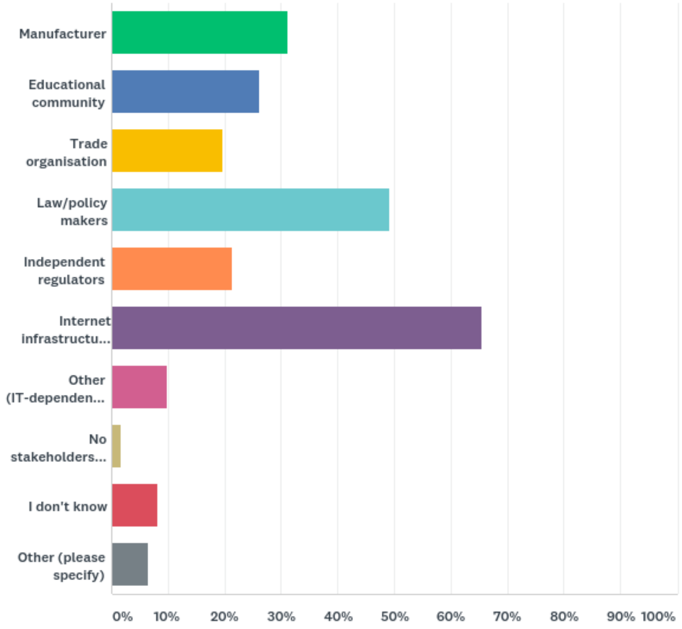


Figure 3. Survey data

Annex 6. Future involvement of stakeholders



Q42 Which stakeholders in general need to be (more) involved in order have internet standards deployed in a faster manner? [Please choose a maximum of three stakeholder groups]

Figure 4. Survey data

Annex 7. Dutch approach on multistakeholder cooperation

Undoubtedly more initiatives are going on in the world than this project could ever digest. Unfortunately, within the given time frame the scope of action was limited. As you saw, most examples in this report are Dutch. This may in part be explained by the fact the authors are Dutch, but does not explain why non-Dutch participants, were not forthcoming with initiatives in their respective countries.

Desk research compensates in part for this, although there at times is a language barrier. The available time does not allow for extensive comparisons. Despite these facts several indicators reveal that The Netherlands has a role as the provider of successful initiatives and examples.

One aspect has become extremely clear though. The polder model is often mentioned as being unique. Although it has been under attack in The Netherlands recently, where cyber security is concerned it allows for making steps that appear harder to make elsewhere in the world. Looking at many initiatives in The Netherlands it shows that ECP, the Dutch national platform for the information society[155], often is involved as a neutral partner providing a secretariat and neutral terrain for and in between the different stakeholder communities. The neutral environment creates the circumstances in which the different stakeholders, despite their differences or even competitiveness and individual priorities, can discuss common internet governance challenges that need to be solved. When successful, after months or even a few years of talks, the outcomes know a solid foundation and commitment from the organisations / stakeholders participating in the process.

Initiatives like e.g. Internet.nl, Abuse Hub, Secure Software Alliance and others can be promoted actively abroad as potential solutions for other countries. Comparative study shows that the eGovernment services in The Netherlands are the best secured in Europe[156]. The ‘Pas-toe-leg-uit’ (apply or explain) list of Standardisation Forum in combination with other efforts like the mentioned ECP programs and Internet.nl may be a reason for this positive position.

Although not a part of this project, the Global Forum on Cyber Expertise[157] could become involved in the dissemination of the recommendations and the way forward after this report. Perhaps even projects could be defined within this context, taking off from the findings here.

[155] https://ecp.nl/
[156] Internet.nl & de eGovernment benchmark
[157] https://www.thegfce.com/

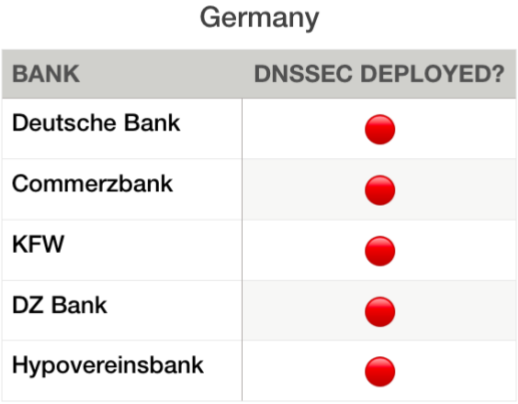
This way of working allows The Netherlands, although of course not uniquely so, to be a front runner where providing solutions and ways forward is concerned. As cyber security issues will only grow in the coming years, perhaps even decades, the ECP / polder model could become an export product to advocate actively to partners abroad as it clearly leads to results that are actively implemented and supported across the board.

In fact, in this context business cases and positive incentives were created, allowing all involved to make the next step. The question to be answered is, can this model play a role where the deployment of internet standards is concerned? It would prevent governments having to legislate in a general sense.

What a process like this also lays bare, is when consensus cannot be reached between stakeholders, the last resort, legislation, is obvious and can be used in further negotiations as an unavoidable outcome. Another recognised pressure point society can provide towards the creation of a positive business case.

Annex 8. DNSSEC in the banking sector

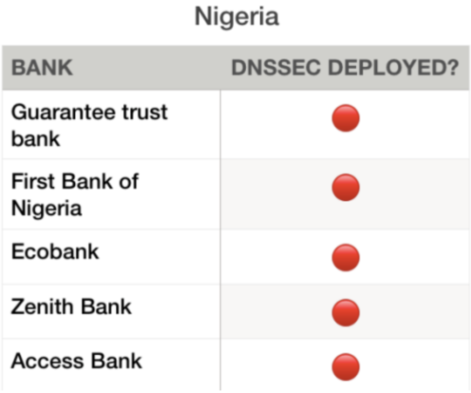
Result of internet.nl's DNSSEC-test for the home pages of the major banks of major economies around the world[158].



Germany

BANK	DNSSEC DEPLOYED?
Deutsche Bank	🔴
Commerzbank	🔴
KFW	🔴
DZ Bank	🔴
Hypovereinsbank	🔴

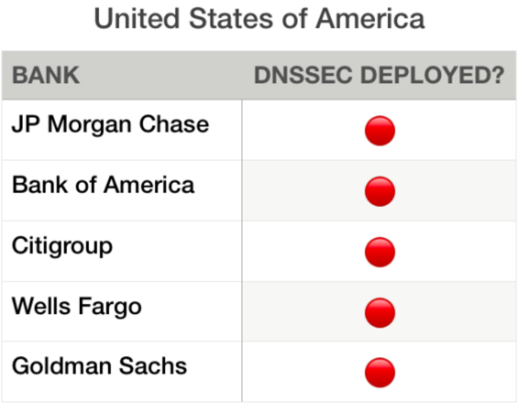
Figure 5. Banks Germany



Nigeria

BANK	DNSSEC DEPLOYED?
Guarantee trust bank	🔴
First Bank of Nigeria	🔴
Ecobank	🔴
Zenith Bank	🔴
Access Bank	🔴

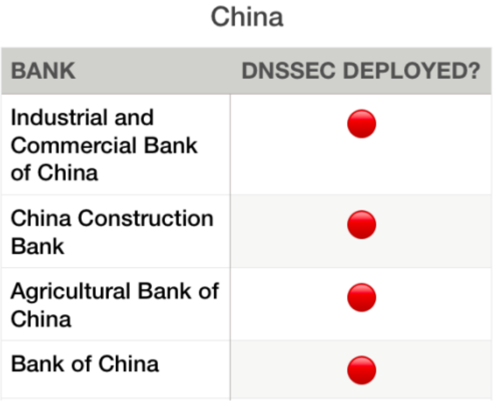
Figure 6. Banks Nigeria



United States of America

BANK	DNSSEC DEPLOYED?
JP Morgan Chase	🔴
Bank of America	🔴
Citigroup	🔴
Wells Fargo	🔴
Goldman Sachs	🔴

Figure 8. Banks USA



China

BANK	DNSSEC DEPLOYED?
Industrial and Commercial Bank of China	🔴
China Construction Bank	🔴
Agricultural Bank of China	🔴
Bank of China	🔴

Figure 7. Banks China

[158] www.internet.nl (accessed 22-01-2020)