Journal of Network and Systems Management (Springer)

Special Issue on a Responsible Internet

Submissions due: Sep 30, 2021

[We encourage early submission, please check the schedule below]

We solicit papers that contribute to a responsible Internet, a novel security-by-design extension of the Internet (or future networks) that increases the digital sovereignty of modern societies.

Addressing a societal problem: increasing dependency, declining sovereignty

Societies **increasingly depend** on digital services because they improve the wellbeing of citizens and contribute to a thriving economy, amongst others. At the same time, however, there are growing concerns around the world that our societies are losing control over these dependencies and as a result face a **decline in their "digital sovereignty"**, in particular in regard to the emerging importance of safety-critical services such as smart energy grids, self-organizing supply chains, and networked health services.

The reason for these concerns is that the underlying computer systems and networks (e.g., algorithms, DNS services, and network equipment) are increasingly manufactured or operated elsewhere, while organizations and individuals have limited insight into, and control over how their businesses and lives depend on those systems. This limitation reduces the ability of our societies to autonomously decide and act on how they use, depend on, and set up their digital infrastructure, which may ultimately pose a risk to public values such as safety, transparency, privacy, and democracy.

Digital sovereignty is highly relevant and urgent but does not consider the Internet infrastructure

Declining digital sovereignty is a widely acknowledged and urgent problem and the subject of an intensifying public debate that takes place at various levels. For example, "responsible AI" is a multi-disciplinary paradigm to make the decisions of AI algorithms more transparent and explainable, thus shifting control to end-users and other stakeholders and away from the giant corporations that often develop and operate these algorithms. Similarly, Europe is developing the federated cloud service "GAIA-X" that aims to improve the region's data sovereignty, and is developing various policies for areas such as 5G cellular access networks and the Internet of Things. Also, the Australian government will actively track the dependencies of the country's critical IT infrastructure, for instance in terms of composition of supply chains and outsourcing of IT activities.

However, these discussions largely overlook the **Internet infrastructure**: the technical substrate that enables applications to communicate across networks and administrative domains and upon which everything else (policy making, services, AI, data) depends.

A new security paradigm: the responsible Internet

One possible way to fill this gap is through the concept of a responsible Internet [1], a novel **security paradigm** that aims to solve the problem of declining digital sovereignty by **enhancing the original set of design goals of the Internet protocol suite** with three new ones: transparency, accountability, and controllability. **Transparency** is about the Internet enabling users to inspect its internal workings, for instance to discover which network operators (e.g., ISPs, data centers, and DNS operators) potentially handle their data flows and what the properties of these operators are (e.g., in terms of their security reputation, applicable jurisdiction, and relations with other operators). **Accountability** is about users being able to verify that these details are accurate, and **controllability** involves users leveraging these insights and telling the network to handle their data flows in a specific way (e.g., by allowing them to only pass through network operators with a certain security posture or within a certain jurisdiction).

With a responsible Internet, users thus have more insight into, and control over how they depend on the network. This is a **fundamentally different way of communicating** over the Internet than today that benefits providers of safety-critical services (e.g., energy grids, transport systems, and health care services) as well as all kinds of other users (e.g., policy makers, network operators, and individuals).

The responsible Internet will continue to follow the current Internet's **open, bottom-up and multi-stakeholder nature**. The sovereignty it provides allows service providers and individuals to be more in control of their dependencies on the Internet infrastructure. Note that the sovereignty we have in mind is explicitly not about creating government-controlled or even isolated national networks, nor is it about excluding technologies from specific regions.

Research results that contribute to a responsible Internet

The transformational nature of a responsible Internet introduces many new research challenges, amongst others in the area of network and systems management. The goal of this JNSM special issue on a responsible Internet is to enable the research and operational communities to obtain an **overview of recent research results** that address these challenges.

Authors may draw inspiration from [1], which outlines a first potential solution to realize the three design goals of a responsible Internet and discusses a set of associated research challenges and potential starting points.

We solicit both papers that build on the notion of a responsible Internet in [1] and papers on technical solutions and their implementation that address the problem of digital sovereignty for the Internet infrastructure in a different way.

Although our focus is technical, we particularly welcome submissions that **complement technical results by considering societal dimensions** (e.g., business or governance implications).

Topics of interest

We solicit original work on topics such as:

- Real-world services that benefit from a responsible Internet
- Trust and sovereignty requirements that these services impose on the Internet
- Languages for expressing trust and sovereignty requirements
- Languages for describing the properties of network operators and their infrastructure
- Security-driven inter-domain and intra-domain routing protocols
- Remote attestation systems and protocols for network nodes (e.g., routers and switches)
- Large-scale measurement systems that map the properties of network operators
- Interoperability of measurement systems
- Dynamic path composition using path segments and VNFs
- Data and control plane-programmable inter-domain networks
- Mechanisms to balance transparency and security
- Verification of network paths used, both intra and inter-domain ("proof-of-path")

Please contact the guest editors if you are uncertain if your submission is in scope for this special issue.

Submission schedule

We use an "open" submission schedule, which means that you can **submit your paper at any time** before we close the call (see below) and that we will start the review process right after receiving the submission.

- Call closes: Sep 30, 2021
- Revision notification: 2 months after submission

- Revised paper due: 1.5 months after the revision notification
- Final notification: 1 month after the revised paper notification
- Expected publication of the special issue: first quarter of 2022 (early accepted papers will be accessible online before the deadline)

Submission format and review guidelines

Submitted manuscripts must be written in English and must not exceed **30 pages in Springer LNCS format**. Your paper must describe original research not published or currently under review by other journals or conferences. Parallel submissions will not be accepted.

All submitted papers, if relevant to the theme and objectives of the special issue, will go through an external peer-review process. Submissions should (i) conform strictly to the Instructions for Authors available on the JNSM website and (ii) be submitted through the Editorial Management system available at http://www.editorialmanager.com/jons.

Further reading

More on the design goals of a responsible Internet, its advantages for different types of users, and a possible way to realize these goals can be found in this paper:

[1] C. Hesselman, P. Grosso, R. Holz, F. Kuipers, J. Hui Xue, M. Jonker, J. de Ruiter, A. Sperotto, R. van Rijswijk-Deij, G. C. M. Moura, A. Pras, and C. de Laat, "A Responsible Internet to Increase Trust in the Digital World", Invited paper, Journal of Network and Systems Management (JNSM), special issue on "Future of Network and Service Operations and Management: Trends, Developments, and Directions", October 2020, https://link.springer.com/article/10.1007/s10922-020-09564-7

Guest editors of the special issue

Cristian Hesselman (chair), SIDN Labs and University of Twente, the Netherlands
Email: cristian.hesselman@sidn.nl

Paola Grosso, University of Amsterdam, the Netherlands
Email: p.grosso@uva.nl

Ralph Holz, University of Twente, the Netherlands
Email: r.holz@utwente.nl

Fernando Kuipers, Delft University of Technology, the Netherlands
Email: F.A.Kuipers@tudelft.nl

Janet Hui Xue, Universität Duisburg-Essen, Germany, and Wolfson College, University of Oxford, UK
Email: hui.xue@wolfson.ox.ac.uk

Abhishta Abhishta, University of Twente, the Netherlands
Email: s.abhishta@utwente.nl

Diego Perino, Telefonica, Spain
Email: diego.perino@telefonica.com

Anne Remke, University of Münster, Germany
Email: anne.remke@uni-muenster.de