Scandinavian Journal of Information Systems

Volume 35 | Issue 2 Article 4

12-31-2023

The Hijacking of the Scandinavian Journal of Information Systems. Reflections and commentary

Sune D. Müller
University of Oslo, sunedm@ifi.uio.no

Anna Abalkina
Freie Universität Berlin, anna.abalkina@fu-berlin.de

Reflection note

The Hijacking of the Scandinavian Journal of Information Systems

Reflections and commentary

Sune Dueholm Müller
University of Oslo
sunedm@ifi.uio.no

Anna Abalkina
Freie Universität Berlin
anna.abalkina@fu-berlin.de

In this paper we, Sune Dueholm Müller and Anna Abalkina, offer complementary perspectives on the recent hijacking of the Scandinavian Journal of Information Systems (SJIS). It is the perspectives of an insider, the editor-in-chief (Sune Dueholm Müller), and an outsider, Anna Abalkina, who is a social scientist specializing in the study of scientific misconduct, including journal hijacking.

An insider's reflections

I am ending my tenure as editor-in-chief with proverbial battle scars but full of optimism and hope for the future. Much to my surprise and chagrin, this past year has been mostly about combating the SJIS hijacking.

Wikipedia offers a succinct definition of Journal hijacking: "Journal hijacking refers to the brandjacking of a legitimate academic journal by a malicious third party" (Wikipedia, 2023). Typically, this third party sets up "a counterfeit website that pretends to be the website of a legitimate scholarly journal. The website creators then solicit manuscript submissions for the hijacked version of the journal, pocketing the money" (Beall, 2023). To this definition Retraction Watch adds that "hijacked journals mimic legitimate journals by adopting their titles, ISSNs, and other metadata” (Retraction Watch, n.d.).

In February, I discovered that cybercriminals had hijacked our brand and had established a fraudulent website posing as the legitimate home of the journal. The cybercriminals are still in business, and I have been unable to stop their operation despite concerted efforts. As of December 29th, the fake SJIS had published more than 250 articles across three issues. This number compares to the handful of papers that SJIS publishes twice a year. I have published a paper in Information Systems Journal (ISJ) that details the events in the aftermath of my discovery (Müller & Sæbø, 2023). The paper is open access and can be downloaded here: https://onlinelibrary.wiley.com/doi/full/10.1111/isj.12481

In this reflection note, I want to describe why it is such an intractable problem, discuss response strategies, and share my outlook on the future. I have invited Anna Abalkina, a research fellow at Freie Universität Berlin and an expert on hijacked journals, to comment on my experiences and offer her perspectives.

Today, the distribution of and access to academic or scientific knowledge is intrinsically bound to technology platforms. As researchers, we search for and download academic literature online. We submit our work through editorial management systems like Bepress’ Digital Commons used by SJIS not to mention the fact that we collaborate and edit our work using Software as a Service tools, including online office and productivity applications like Google Docs and LaTeX Lab. Despite its many benefits, using these tools creates a dependency on the platforms that makes it very difficult to combat journal hijacking. I will elaborate on this based on my experiences in combating the SJIS hijacking.

My priority in combating the SJIS hijacking was to remove the Scopus link to the fraudulent website and reinstate the correct link to our journal website. Cybercriminals had managed to change the link in Scopus, and I know from corresponding with many victims that it was by following this link that they ended up in the clutches of the criminals and paid for fake publications. However, navigating Scopus for contact information, persuading them to act, and achieving the desired changes has been an uphill battle. On December 13th, the correct link was reinstated after I decided to bypass standard reporting and communications channels and reached out to the leadership at Elsevier. I first contacted Elsevier—the company behind Scopus—on February 7th. Unfortunately, this change was mostly symbolic as Elsevier decided to remove all links from journal pages in Scopus in response to the criticism that I and many others, including my co-author Anna Abalkina, have directed against Scopus. My other priority was to ensure that the fraudulent website did not show up when searching the internet for "Scandinavian Journal of Information Systems." However, communicating with the tech giants Google and Microsoft is limited to reporting sites that violate their content and product policies. There is no feedback or guarantee of success. In the SJIS hijacking case, the criminals have responded to the apparent removal from search engines' indexing because of my and others' reporting by cloning the site under a new URL. The criminals seem very experienced in search engine optimization, and, at the time of writing, the fraudulent website appeared among the top 10 hits when searching for the journal using the Google and Bing search engines. PayPal, which facilitated the payment of article processing charges for bogus publications by the fraudulent website, was also contacted but never responded to my request to have the criminals' account seized or shut down. Papers published by the fraudulent website appear on Google Scholar and ResearchGate, and the cybercriminals seem to have established a journal page in ResearchGate that points to the Atma Jaya Catholic University of Indonesia rather than the Association for Information Systems as the legitimate publisher. Google Scholar has not responded to my requests for papers that link to the fraudulent website to be removed. However, the ResearchGate compliance team responded promptly when I contacted them but they referred me to Crossref for a resolution to the problem.

> We rely on Crossref as an authoritative source of information. With that being said, as a starting place, we strongly urge you to reach out to Crossref to address the issues you have raised. This is because, so long as information is being made available by Crossref, including any new records that are added in the future, it will continue to be automatically (re)imported into ResearchGate's systems and reflected on our platform. (Mail from ResearchGate)

Crossref is a nonprofit organization that provides services to the global scholarly research community, including DOI registration to make "research objects easy to find, cite, link, assess, and reuse" (https://www.crossref.org). Crossref was very responsive when I contacted them and promised to contact Atma Jaya Catholic University of Indonesia which has registered DOIs for articles published in the fake journal.

> Once we have confirmation from Atma Jaya, we can move ownership of the title record for Scandinavian Journal of Information Systems in our system from Atma Jaya Catholic University of Indonesia to Association for Information Systems, and then Association for Information Systems can start registering your content with us. (Mail from Crossref)

As of December 29th, 2023, I am still awaiting an update from Crossref.

In my efforts to safeguard and update information about SJIS, I have contacted several other stewards of technology platforms, including:

- SCImago which maintains the SCImago Journal & Country Rank (SJR) (https://www.scimagojr.com)—a portal that includes journals and scientific indicators developed from information in the Scopus database. The information provided by SJR is important because it is used in assessing the scientific influence of scholarly journals like SJIS based on citation data.
- ISSN International Centre which is responsible for the ISSN portal (https://portal.issn.org)—a database of internationally standardized codes (ISSNs) for publications such as journals that facilitates identification and tracking of these publications across databases, systems, and platforms. The information is important because it provides a unique and consistent identifier for publications used in cataloging and distributing, e.g., journal articles. The fraudulent website uses SJIS ISSN to spread the fake papers across platforms.

Common to all these platforms is the difficulty in contacting them and convincing them to change the registered information about the journal. In a way, this is both understandable and reassuring since anyone—including criminals—could otherwise easily change the information. However, this means that it is difficult to solve the problem with the hijacking of the journal because it requires contact with and cooperation from many stakeholders, each with their own processes for handling customer inquiries, and who may—or may not—respond to inquiries from individuals like me who as the editor-in-chief of a journal represent legitimate interests.

In addition to the platforms, I have also reported the fraudulent site to the hosting provider GoDaddy and the following American authorities: the Federal Trade Commission (https://reportfraud.ftc.gov/#), the US Cybersecurity and Infrastructure Security Agency, and the Internet Crime Complaint Center (https://www.ic3.gov/Home/FileComplaint). None of them have responded to my reports of cybercrime.

In summary, several factors make the SJIS hijacking an intractable problem, including the multitude of actors involved with many different interests, the lack of clarity concerning who has the authority to address the problem, and the lack of international governance mechanisms to handle this form of global crime. Despite these difficulties, we have no choice but to try to combat the problem. In the grand scheme of things, it is about disinformation and whether we can trust scientific knowledge. If hijacked journals and predatory publishing practices become widespread, we risk moving towards a future where trust in science and academic publications is weakened. This should also be seen in the context of the widespread use of LLM chatbots, which are trained on data from the internet, including fake articles. What makes me both optimistic and hopeful is, first, my own ability to combat the SJIS hijacking by helping to make the fraudulent website less visible because it does not appear in Scopus. I am also hopeful about having links to the website removed from search engines, ResearchGate, and other places, even though it is a frustratingly slow process. The second is the action possibilities we have as researchers to combat this nascent threat confronting the IS community through defensive and offensive response strategies. These are described in the ISJ paper. The third is the growing awareness of the problem, because of the efforts of, among others, the people behind Retraction Watch (https://retractionwatch.com)—a blog that reports on retractions of scientific papers and a watchdog on scientific misconduct—and researchers like Anna Abalkina whom I have invited to comment on my reflections and offer her perspectives on journal hijacking in terms of response strategies.

An outsider's commentary

In the following, I will put the SJIS hijacking into a larger context of journal hijacking worldwide and offer my perspectives on root causes and how to combat the problem.

Hijacked journals are websites created by cybercriminals who use the title, ISSN, and other metadata of legitimate journals without authorization (Abalkina, 2023a; Jalalian & Dadkhah, 2015; Khosravi & Menon, 2021). There are two primary methods of journal hijacking. The first method involves registering the expired domain of a legitimate journal, which may occur when the original journal moves to a new domain and abandons the old one, ceases publication, or forgets to renew the domain (Bohannon, 2015). The second method involves creating a cloned website of the legitimate journal (Coates, 2022). This method was used in the case of the SJIS hijacking. This strategy is particularly effective against print-only journals, stand-alone journals, journals published in foreign languages, and trade journals, where verifying the authenticity of the website can be challenging. The documentation of hijacked journals began in 2012 (Jalalian & Dadkhah, 2015), and over the past decade, the hijacking of more than 300 journals have been documented (Abalkina, 2023a).

Hijacked journals proliferate when there is pressure on scholars to publish in international journals indexed by bibliographic databases like Web of Science or Scopus, or in whitelisted journals, for example, such as those on the UGC-CARE list in India or the ones recognized by the Higher Education Commission's Journal Recognition System in Pakistan. Hijacked journals share many similarities with predatory journals, both categories mimic reputable journals (Jalalian & Dadkhah, 2015; Lukić et al., 2014), inflate their impact factors (Jalalian & Mahboobi, 2014), and engage in aggressive email marketing (Grudniewicz et al., 2019; Jalalian & Dadkhah, 2015; Lukić et al., 2014). However, unlike predatory journals, which are officially registered, hijacked journals are typically published by anonymous individuals or entities. They represent a form of scam in the publishing industry (Butler, 2013).

Hijacked journals are a lucrative business (Brainard, 2023). Fraudulent websites offer fast publications without peer review in return for fees known as Article Processing Charges (APC). These websites publish hundreds or even thousands of papers until the fraud is exposed or scholars cease payments. The large number of papers raises questions about how newly created, fraudulent websites manage to attract numerous submissions within a short timeframe.

To attract and deceive scholars, hijacked journals employ various strategies. Firstly, they collaborate with broker companies or paper mills to solicit as many submissions as possible. Evidence from the 'International publisher' LLC paper mill indicates the publication of nearly twenty papers in another hijacked journal named Talent Development and Excellence (Abalkina, 2023b). Additionally, the Tanu.pro paper mill (Abalkina & Bishop, 2023; For Better Science, 2023) received an offer in 2021 from the hijacked journal Philosophical Readings to become an official distributor of papers. The offer also included a commercial proposal for APC discounts based on the number of submitted papers (Scientific Publications, 2021).

Secondly, certain hijacked journals have managed to infiltrate Scopus by indexing unauthorized content from a cloned version of a legitimate journal or by compromising the link associated with a legitimate journal on its Scopus profile page (Abalkina, 2023a; Abid & Yousif, 2022; Khosravi & Menon, 2021; Memicevic, 2018; Müller & Sæbø, 2023; Zenthöfer, 2020). This latter scenario occurs when the homepage link in Scopus redirects to a cloned version of the journal. This is what happened in the case of SJIS. 30% of legitimate titles listed in the Retraction Watch Hijacked Journal Checker, a regularly updated list of hijacked journals (Retraction Watch, n.d.), were compromised in Scopus by hijacked journals as of September 2023 (Abalkina, 2023a). The penetration of hijacked journals into Scopus significantly increases the apparent legitimacy of cloned websites for scholars who rely on Scopus to verify the authenticity of journals.

Hijacked journals negatively impact research integrity and academic publishing. First, papers from hijacked journals are often published without peer review and are frequently associated with plagiarism and submissions by paper mills (Abalkina, 2023b).

Second, these papers are indexed in numerous databases, including Google Scholar, Scopus, Web of Science, Dimensions, ResearchGate, ORCID, etc. As a result, they are indexed alongside authentic papers, which makes it difficult to differentiate between papers published by legitimate publishers and those that are not. Some hijacked journals have even registered DOIs for their papers. In the case of SJIS, Crossref registered two DOIs (10.25170/sjis.v35i1 and 10.25170/sjis.v35i1.227 (both hijacked)). Third, these fake papers are cited and included in meta-studies, further infiltrating and corrupting the academic literature. Fourth, papers from hijacked journals are sometimes used for research evaluation, promotion, grant applications, and other academic purposes (Moussa, 2021).

The fake journals negatively impact the editorial processes of legitimate journals. Journal hijacking significantly increases the burden on the editorial boards of genuine journals, due to the rising number of inquiries from scholars deceived by hijacked journals regarding the status of their submitted papers. Additionally, journal hijacking may lead to legal expenses as legitimate journals can be forced to sue to remove papers published on a fraudulent website using the journal's title without permission. Legitimate journals can also be penalized for dishonest activities by the individual or entities behind hijacked journals. For example, there have been cases where Scopus stopped indexing genuine journals due to the infiltration of unauthorized content from hijacked journals, which further tarnished the reputation of these journals (Abalkina, 2023a).

The SJIS hijacking illustrates the extensive efforts an editorial board must undertake to protect its journal from hijacking (Müller & Sæbø, 2023). SJIS is among the 67 journals whose data have been shown to have been compromised in Scopus (Abalkina, 2023a). Hijackers changed the journal's link to a cloned version and succeeded in indexing papers published without peer review on this cloned website. The experience of the journal and its editor-in-chief demonstrates that there are no established procedures for defending a genuine journal, removing unauthorized content from various databases, or shutting down the domain hosting a cloned version of the journal.

This is also one of the few cases where a journal has shared and described its experiences in detail. The SJIS experiences were shared in a separate paper (Müller & Sæbø, 2023) and in a guest post on Retraction Watch (Müller, 2023). Unfortunately, these experiences reveal that enormous efforts are often required to remove unauthorized content or to restore the correct URL of the homepage, and many of these efforts are unsuccessful.

For instance, it took nine months to restore SJIS' homepage link in Scopus after the editor-in-chief noted and reported a link from the bibliographic database to the fraudulent website of the hijackers. However, shortly after the homepage link was restored, Elsevier (Scopus parent company) decided to remove all homepage links from its database due to numerous cases of so-called 'indexjacking,' referring to the infiltration of hijacked journals into bibliographic databases (Scopus, 2023). This extraordinary measure aimed to protect Scopus from compromised links may inadvertently facilitate journal hijacking. Many scholars relied on these homepage links for verification purposes which were available for free (no Scopus subscription required). After the removal of these links, Scopus is advising scholars to verify the authenticity of a journal using the 'view at publisher' option, which is available only to subscribers. It makes the verification of genuine journals more challenging.

Currently, there is limited knowledge of the strategies that journals can employ to effectively prevent journal hijacking or protect the integrity of genuine journals. The SJIS experiences and its efforts to combat the hijacking demonstrate that the scientific and publishing communities should develop guidelines to prevent journal hijacking and strategies to mitigate its consequences. These guidelines and strategies should encompass legal measures and investigations by authorities, as journal hijacking is a form of cybercrime that requires judicial responses. Unfortunately, the organizers of this criminal enterprise remain largely unknown. The publishers are usually anonymous, and the owners of the domains of hijacked journals are kept secret by domain name registrars and hosting companies for privacy reasons. The Information Systems community could significantly contribute to investigating journal hijacking cases, for example, by analyzing the payment details and other data trails of hijacked journals in efforts to expose the fraudsters and help bring them to justice.

Unfortunately, it is impossible to entirely prevent journal hijacking, as fraudulent publishers can easily create cloned websites. However, there are several recommendations that journals like SJIS can follow to minimize risks and mitigate the consequences of this type of cybercrime:

- Journals should employ search engine optimization strategies to ensure visibility in search engine results.
- Journals should diligently manage domain registrations and promptly renew domains to maintain control.
- In the event of a domain change, journals should inform all indexing databases about the transition.

If a journal has already been hijacked it is recommended to inform the scientific community about the hijacking on the website of the journal.

I advise all journals within Information Systems and other disciplines to follow these recommendations, and not least take advantage of the knowledge and experience that the SJIS editor-in-chief has gained over the last year. Unfortunately, following these recommendations will not fully mitigate the consequences of journal hijacking. However, the reporting on the SJIS hijacking has helped raise awareness of the threat to the scientific community posed by journal hijackers and it has initiated discussions of strategies that can be leveraged in response to journal hijacking. Going forward, we need to continue these discussions, and the scientific and publishing communities should engage in dialogue around preventive and mitigation measures, including establishing trust markers for genuine journals.

Bibliography

Abalkina, A. (2023a). Challenges posed by hijacked journals in Scopus. *Journal of* the *Association for Information Science and Technology*.

Abalkina, A. (2023b). Publication and collaboration anomalies in academic papers originating from a paper mill: Evidence from a Russia-based paper mill. *Learned Publishing*, *36*(4), 689-702.

Abid, H., & Yousif, E. (2022). Hijacked journals: Tips for young researchers, to detect and avoid them. *Baghdad Journal of Biochemistry and Applied Biological Sciences*, *3*(4), 232-236.

Beall, J. (2023). Hijacked journals. Retrieved on 28 December 2023 from Beall's List of Potential Predatory Journals and Publishers: https://beallslist.net/hijacked-journals/

Bishop, D., & Abalkina, A. (2023). Paper mills: a novel form of publishing malpractice affecting psychology. *Meta-Psychology*, *7*, MP.2022.3422.

Bohannon, J. (2015). How to hijack a journal. *Science*, *350*(6263), 903-905.

Brainard, J. (2023). Leading scholarly database listed hundreds of papers from 'hijacked' journals. *Science*, 5 Dec 2023.

Butler, D. (2013). Sham journals scam authors: Con artists are stealing the identities of real journals to cheat scientists out of publishing fees. *Nature*, *495*(7442), 421-422.

Coates, A. (2022). Academic journals' usernames and the threat of fraudulent accounts on social media. *Learned Publishing*, *35*(2), 140-148.

For Better Science (2023). Ukrainian papermills—symptom, not a cause. For Better Science, Sep 4, 2023. Retrieved on 25 December 2023 from https://forbetterscience.com/2023/09/04/ukrainian-papermills-symptom-not-a-cause/

Grudniewicz, A., Moher, D., Cobey, K. D., Bryson, G. L., Cukier, S., Allen, K., … Lalu, M. M. (2019). Predatory journals: No definition, no defence. *Nature*, *576*(7786), 210-212.

Jalalian, M., & Dadkhah, M. (2015). The full story of 90 hijacked journals from August 2011 to June 2015. *Geographica Pannonica*, *19*(2), 73-87.

Jalalian, M., & Mahboobi, H. (2014). Hijacked journals and predatory publishers: Is there a need to re-think how to assess the quality of academic research? *Walailak Journal of Science and Technology (WJST)*, *11*(5), 389-394.

Khosravi, M., & Menon, V. (2021). Reliability of hijacked journal detection based on scientometrics, altmetric tools, and web informatics: A case report using Google Scholar, Web of Science, and Scopus. *Security and Communication Networks*, *2021*, 1631496.

Lukić, T., Blešić, I., Basarin, B., Ivanović, B. L., Milošević, D., & Sakulski, D. (2014). Predatory and fake scientific journals/publishers: A global outbreak with rising trend: A review. *Geographica Pannonica*, *18*(3), 69-81.

Memicevic, H. (2018). In Web of Science we trust—A case of a hijacked journal indexed in Scopus. ISSI Newsletter, *14*(1), 1-5.16.

Moussa, S. (2021). Journal hijacking: Challenges and potential solutions. *Learned Publishing*, *34*(4), 688-695.

Müller. S.D. (2023). My journal was hijacked: An editor's experience. Retrieved on 25 December 2023 from https://retractionwatch.com/2023/11/03/my-journal-was-hijacked-an-editors-experience/

Müller, S. D., & Sæbø, J. I. (2023). The 'hijacking' of the Scandinavian Journal of Information Systems: Implications for the information systems community. *Information Systems Journal*, 1-20.

Retraction Watch (n.d.) The Retraction Watch Hijacked Journal Checker. Retrieved on 28 December 2023 from https://retractionwatch.com/the-retraction-watch-hijacked-journal-checker/

Scientific Publications. (2021). Journal 'Philosophical Readings' now has a clone. Be careful! (У журнала «Philosophical Readings» появился клон. Будьте осторожны!). Retrieved on 25 December 2023 from https://spubl.com.ua/ru/blog/u-zhurnala-philosophical-readings-poyavilsya-klon-budte-ostorozhny

Scopus (2023). Scopus will remove the Source Homepage links from all Source details pages. Retrieved on 25 December 2023 from https://blog.scopus.com/posts/scopus-will-remove-the-source-homepage-links-from-all-source-details-pages

Wikipedia. (2023). Retrieved on 28 December 2023 from https://en.wikipedia.org/wiki/Journal_hijacking

Zenthöfer, J. Alles für den Zitationsindex. *Frankfurter Allgemeine Zeitung*, 17 Jul 2020.