bjoern.brembs.blog

Is the SNSI the new PRISM?

Björn Brembs

Published October 26, 2020

Citation

Brembs, B. (2020, October 26). Is the SNSI the new PRISM?. *Bjoern.brembs.blog*. https://doi.org/10.59350/wd8jd-gs019

Keywords

Science Politics, PRISM, Publishers, Sci-hub, SNSI

Just before Christmas 2019, the Washington Post reported, based on "people familiar with the matter", that the US Justice Department were investigating the Sci-Hub founder Alexandra Elbakyan for potentially "working with Russian intelligence to steal U.S. military secrets from defense contractors". Besides such a highly unusual connection, the article also reiterated unsubstantiated (but mainly circulated by publishers) allegations that access to scholarly journals was obtained via her 'hacking' skills. The article also cited a "former senior U.S. intelligence official" that he believed Elbakyan was working with the Russian foreign intelligence service GRU. Apparently, the investigation had been ongoing since 2014, but now, in 2020, there is still no publicly available evidence as to what this investigation has been able to find.

And yet, despite no evidence, on the very next day after the Washington Post story, Elsevier was all too happy to find their oft-repeated but little-believed claims of Sci-Hub being dangerous vindicated and exclaimed "This represents a threat to academic institutions". Elsevier, after winning a lawsuit that failed to materialize any of the millions it sought, finally had external support to bolster their claims that Sci-Hub was not only a threat to their bottom line, but to research integrity!

Less than two months later, Nick Fowler, chief academic officer at Elsevier, announced the new *Scholarly Networks Security Initiative* (SNSI), under the title "Working together to protect from cyber attacks". Fowler was assisted by SpringerNature chief publishing officer Steven Inchcoombe. Both introduced themselves as co-chairs of SNSI. One aspect mentioned in the article was that "Awareness of the damage Sci-Hub is inflicting on institutions and academia needs to be increased." The idea being that publishers and institutional libraries work together to fight a common enemy.

This public relations aspect of the SNSI is what needs to receive special attention. On the face of it, Sci-Hub is an enabling technology: before Sci-Hub, scholars needed subscriptions to access the scholarly literature; now, subscriptions have become optional. In many countries, this has led to new initiatives and consortia finally toughening their stance in library-publisher negotiations. What in the previous three decades was a walk in the park, followed by ever climbing profit margins now stands to be a tough negotiation. Sci-Hub thus has had opposite effects on libraries and publishers: while libraries need not fear lapses of access as much as previously, allowing them to be bolder in their negotiations, publishers wonder why anybody should pay for their offerings at all, if their customers can have all the scholarly content of the world for free.

When it turned out that the lawsuits against Elbakyan would neither lead to any damages being paid nor have a deterring effect on libraries or their patrons, and when initiatives asking for a tougher stance against publishers garnered more and more support, publishers devised a new strategy. They would try and paint Sci-Hub not only as a threat for them, but also for the libraries. Rumors started spreading unsubstantiated claims that Sci-Hub had obtained their login-credentials, with which they were populating their databases, not by donations, but by phishing attacks. As there was no evidence, there was little uptake or discussion. One may assume that with Sci-Hub being around since 2011, noticeable consequences on library

behavior starting around 2012/13, by 2017/18, when the phishing rumors failed to gain traction, publishers must have been fairly frustrated that their usual power over academics seemed on the decline for the first time in decades.

Perhaps the feeling of frustration was similar around 2005, when the Open Access movement, invigorated by the Budapest (2001) and Berlin (2003) declarations, continued to garner steam. Also then, the publishers' attempts at painting Open Access to scholarly works as a threat to research integrity failed to rouse support and slow the momentum of the OA movement. Just before the launch of the NIH OA mandate in the US, the American Association of Publishers (AAP) decided they needed something that would really get their message across and in 2006 started the Partnership for Research Integrity in Science and Medicine (PRISM) Coalition*. They hired "the pit bull of public relations", Eric Dezenhall, to create a smear campaign hat would strive to equate public access with junk science. In particular with regard to OA mandates, part of the plan was for publishers to partner with anti-science organizations, which shared their anti-government sentiment. The aim was to bring institutions on board to save research integrity together with the publishers.

Thus, in both instances, public access to scholarly works (whether via OA or Sci-Hub) posed only a threat to publishers and in both instances, the publishers sought to paint themselves as chiefly concerned not about their bottom line but about "research integrity". Compare the statement on the PRISM website:

> *The Partnership for Research Integrity in Science and Medicine (PRISM) was formed to advocate for policies that ensure the quality, integrity, and economic viability of peer-reviewed journals.*

with statements on the SNSI site:

> *Scholarly Networks Security Initiative (SNSI) brings together publishers and institutions to solve cyber-challenges threatening the integrity of the scientific record, scholarly systems and the safety of personal data.*

This past week, these public relations efforts were dialed up a notch or ten to a whole new level. At an SNSI webinar entitled „Cybersecurity Landscape – Protecting the Scholarly Infrastructure", hosted by two Elsevier employees, one of the presenters suggested to „develop or subsidize a low cost proxy or a plug-in to existing proxies" in order to collect user data. That user data, it was explained, could be analyzed with an "Analysis Engine" to track biometric data (e.g., typing speed) or suspicious behavior (e.g., a pharmacology student being suspiciously interested in astrophysics). The angle towards Sci-Hub was confirmed by the next speaker, an Ex-FBI agent and security analyst.

Considering the track record of academic publishers, this reeks strongly of PR attempts to 'soften the target', i.e., to make installing publisher spyware on university servers sound less outrageous than it actually is. After the PRISM debacle, the publishers now seem to have learned from their PR mistakes. This time, there is no 'pitbull' around. This time, there is only a

strange article in a major newspaper, a shady institute where it appears hard to find out who founded it, who is running it and who funds it.

SNSI is an apparent PR project aimed at compromising, not strengthening, network security at research institutions. However, unlike with PRISM, this time the PR effort may pay off.

---

* It has to be noted that one of the AAP publishers in the PRISM Coalition was Elsevier, who had so much disdain for research integrity that they had published a nine fake journals from 2000 until 2005. In other words, in one year, they stop publishing their fake journals, in the next, they join a PR campaign in which research integrity is the central tenet.