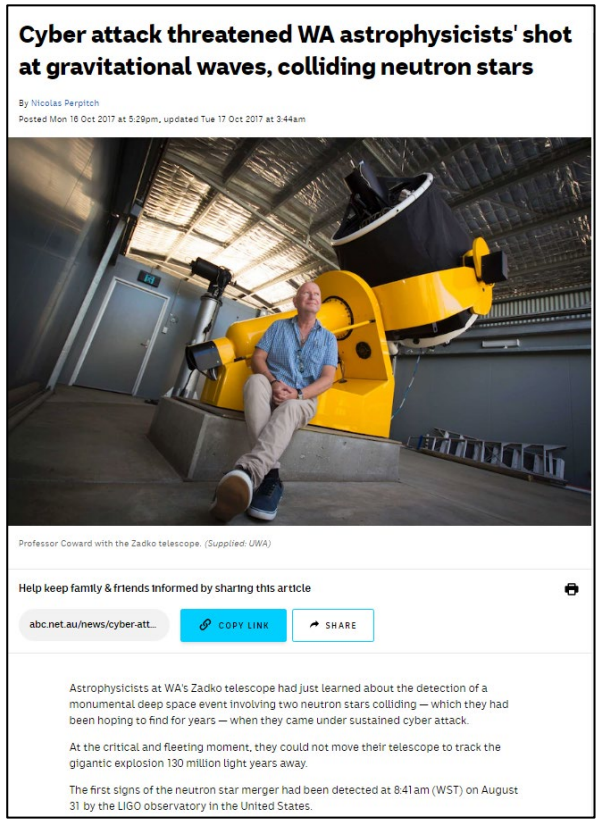
Laboratory Data Security

- Research data of regulated science is guided by compliance, *e.g.*, HIPPA, FISMA, NIST 800-171
- Open science is not guided by compliance
- Data security is important for **Productive**, **Trustworthy** and **Reproducible** science
- Ransomware encrypts the data and sell it back to user.
- Running science on a hacked computer?



Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

By Nicolas Perpitch

Posted Mon 16 Oct 2017 at 5:29pm, updated Tue 17 Oct 2017 at 3:44am

Professor Coward with the Zadko telescope. *(Supplied: UWA)*

Help keep family & friends informed by sharing this article

abc.net.au/news/cyber-att... COPY LINK SHARE

Astrophysicists at WA's Zadko telescope had just learned about the detection of a monumental deep space event involving two neutron stars colliding — which they had been hoping to find for years — when they came under sustained cyber attack.

At the critical and fleeting moment, they could not move their telescope to track the gigantic explosion 130 million light years away.

The first signs of the neutron star merger had been detected at 8:41am (WST) on August 31 by the LIGO observatory in the United States.

https://www.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-team-look-at-colliding-neutron-stars/9055816

NEWS | IN DEPTH

is rare for everything to work perfectly [the] first time," the university writes, "and the introduction of tissue engineered treatments is no exception." As to the animal studies, UCL doesn't address many of the issues raised by Murray and Lévy but says its researchers "have done as much as they can already to show safety and efficacy in animals," and further animal work would be unethical.

Other scientists say the jury is still out on the effects of stem cells in these kinds of grafts. "The impact of seeded cells for us is unclear at this point," says Tendy Chiang, a pediatric otolaryngologist at Nationwide Children's Hospital and The Ohio State University in Columbus, who is conducting preclinical research into tissue-engineered trachea transplants.

John Rasko, a clinical haematologist and pathologist at Royal Prince Alfred Hospital in Sydney, Australia, says U.K. funding bodies have a "declared enthusiasm" for research on stem cell therapy. But given the issues raised by critics, "to now have this substantial investment in Birchall and others' trials in the U.K. is something of concern," says Rasko, who was recently elected president of the International Society for Cellular Therapy but says he's speaking in a personal capacity. "I just don't see why there's a need to rush into these things until clear evidence is brought to bear," he adds.

The parliamentary committee is expected to publish its report in the next few months, but it appears unlikely to render any judgment about Birchall's trials. A source at the committee says the inquiry's intention is to examine how institutions respond to allegations of research misconduct, rather than to investigate any particular case.

What will happen to the studies remains unclear. In the wake of UCL's 2017 inquiry, the INSPIRE consortium decided to conduct a further risk assessment. As a result, say spokespeople for the Cell and Gene Therapy Catapult, a nonprofit center that serves as the trial's sponsor, the group has decided to "gather more data" and "will only recommend the restart of any trials ... if supported by expert opinion with regulatory and ethical approval." UCL did not respond to questions about the future of the RegenVox trial, but for now it remains listed as "suspended" on the university's website.

Murray says Macchiarini and Birchall both rode on the high hopes for stem cells. Media stories about their operations—sometimes with photos of patients taken shortly after surgery—projected an air of success that blinded even respected institutes and funders to potential flaws in the research, she says: "Once people were seeing pictures of the patients, maybe no one's really looking at the hard evidence so much anymore."

CYBERSECURITY

U.S. blames 'massive' hack of research data on Iran

Targets included nearly 8000 professors in 22 countries

By Jon Cohen

A "massive and brazen cyberassault" revealed last week by the U.S. Department of Justice (DOJ) showed that academics are easy targets for hacking. In "one of the largest state-sponsored hacking campaigns" it has ever prosecuted, DOJ alleges that nine Iranians working on behalf of the Islamic Revolutionary Guard Corps stole data from 7998 professors at 320 universities around the world over the past 5 years.

The indictment, filed by a federal grand jury in New York City and unsealed on 23 March, alleges that the hackers pilfered 31.5 terabytes of documents and data, including scientific research, journals, and dissertations. Their targets also included the United Nations, 30 U.S. companies, and five U.S. government agencies. The indictment does not name the hacked academic institutions or companies, but it notes that the victims included academic publishers, a biotechnology company, and 11 technology companies.

"This is not an isolated breach—it's hundreds if not thousands of breaches," says Anthony Ferrante, who heads cybersecurity at FTI Consulting in Washington, D.C., and formerly worked as a cyber expert for the White House's National Security Council. Ferrante says academia is particularly vulnerable because of its open, collaborative ethos. "It really becomes a target for malicious cyberactivity."

The hacks came to light through investigations by the Federal Bureau of Investigation and reports from victims. "The hackers targeted innovations and intellectual property from our country's greatest minds," said U.S. Attorney Geoffrey Berman of the Southern District of New York, where the indictment was filed.

Bahram Ghasemi, spokesperson for Iran's Ministry of Foreign Affairs, countered that the accusations were false and "yet another clear sign of the U.S. ruling elite's inherent hostility and enmity towards the Iranian nation." Some U.S. cyber and policy analysts also see political motivations behind the indictment and suggest the actual harm was modest.

According to the indictment, the attack targeted 3768 professors at 144 U.S. universities and stole data that cost the institutions about $3.4 billion to "procure and access." The accused allegedly set up an institute in Iran called Mabna that coordinated and paid for the hacks. The institute, the indictment says, aimed to "assist Iranian universities, as well as scientific and research organizations, to obtain access to non-Iranian scientific resources." The stolen data were sold through two websites, Gigapaper and Megapaper.

The indictment says the university breaches involved "spearfishing," in which the accused sent emails that tricked targets into providing their login credentials. The emails supposedly came from professors who had read articles by the targets and asked for access to more of their work, helpfully providing links. Clicking a link took the victim to a fake internet domain that resembled their own university's website and asked them to log in.

> *"College professors are like shooting fish in a barrel."*
> **Max Kilger**, University of Texas

With the harvested credentials, documents and other resources were easy pickings. "College professors are like shooting fish in a barrel," says Max Kilger, a social psychologist at University of Texas in San Antonio who studies motivations of cyberterrorists. "For the most part, they're pretty unassuming and they leave valuable data on personal machines and university machines that aren't very well protected." (For the private sector, the indictment says hackers used "password spraying," cracking into accounts with commonly used passwords.)

The charges against the accused include wire fraud, aggravated identity theft, and conspiracy to commit computer intrusions. The U.S. Department of the Treasury separately announced sanctions against the alleged perpetrators. They "are no longer free to travel outside of Iran without the fear of being arrested and extradited to the United States," Berman said. "The only way they can see the rest of the world is through their computer screen, but now stripped of their greatest asset, anonymity."

1450 30 MARCH 2018 • VOL 359 ISSUE 6383 sciencemag.org SCIENCE

Published by AAAS

Cohen, J., *Science* **2018**, *359* (6383), 1450-1450.

1. **Secure Storage Best Practices**
   - Do not expose research infrastructure to the Internet
   - Encrypt sensitive data transmitted over a network
   - Develop a central data backup service
   - Destroy data that is no longer needed
2. **Encryption**
   - Highest level of data encryption for rest and transit data
3. **Commercial Cloud Services**
   - Use cloud services with two-factor authentication
4. **Hardware Security**
   - Use up-to-date OS with modern anti-virus software
   - Systems with old OS should be free of IP addresses
   - Only authorized employees should use peripheral devices
5. **Application Security**
   - Utilize two-factor authentication, passwords and role-based access control
6. **Network Security**
   - Use Standard security measures like SSL
   - Use Laboratory information management systems (LIMS)
7. **Personnel Security**
   - Background checks, training and compliance

- osp.od.nih.gov/wp-content/uploads/NIH_Best_Practices_for_Controlled-Access_Data_Subject_to_the_NIH_GDS_Policy.pdf
- irtsectraining.nih.gov/publicUser.aspx

Stony Brook University

Center for Adaptive Flaws into Features