Published on 01 February 2022 in ISS Today

By Karen Allen
Consultant, ISS Pretoria

Print

Share this:

Keeping the humanitarian sector in Africa safe from digital threats

The recent Red Cross cyber-attack is a reminder that emerging tech comes with risks.

Last month's cyber-attack on the International Committee of the Red Cross and its affiliated bodies showed that the humanitarian community isn't immune from cybercrime. Given that Africa is a focal point for many humanitarian operations and is experiencing rising rates of cybercrime across all sectors, this is especially sobering.

It's shone a spotlight on the reality that although emerging technologies have positively transformed how aid is delivered, there are also potential harms. Many Red Cross operations are conducted in Africa – e.g. in the Sahel, Ethiopia, Chad and the Democratic Republic of the Congo. So for the continent it's a reminder that tech without due consideration of the risks could expose many vulnerable people to harm.

The breach saw the personal data of nearly half a million vulnerable people being exposed globally. As more unfolds on the incident, it's becoming clearer that the Red Cross was almost certainly singled out for attack. The motivation is yet to be established.

The hackers targeted the organisation's servers stored at a Switzerland-based facility. 'It was sophisticated enough that it wasn't just a 15-year-old computer hacker having some fun,' said Delphine van Solinge, an adviser to the Red Cross on digital risks in the humanitarian sphere. 'It seemed to be well organised, well planned and rolled out, but we cannot say who was behind it and why they did it.'

COVID-19 and multiple cyber-attacks on institutions such as the World Health Organization have underscored cyber threats to the aid world. Like governments, businesses, universities, and multilateral institutions, humanitarian players must temper the dash to embrace emerging tech and soberly assess potential risks.

> Africa is a focal point for many humanitarian operations and is experiencing rising rates of cybercrime

The digital revolution has helped provide real-time data during crisis or conflict. But if this information falls into the wrong hands it can be potentially life-threatening, or at the very least distressing.

'It is very difficult to speculate on the intention of the perpetrator in this attack,' says Van Solinge, 'but the individuals the [Red Cross] works with are often fleeing conflict and seeking to be re-united with families overseas. Revealing their identities or movements may put their safety in jeopardy.'

It may be used for politically expedient purposes. There's also a market for personal data. Stolen identities are used to perpetrate fraud, extortion and other crimes. For these reasons, along with other ethical considerations, in the wake of the breach, the Red Cross appealed for people not to share, sell, or leak the information.

Unauthorised access to the same data held physically would also have been considered a serious breach. However the digital dimension to this intrusion enables highly sensitive data to be distributed quickly. Also, once personal records are released publicly into cyberspace, they're hard to remove.

Like other humanitarian players, the Red Cross is being forced to review its cyber security measures and consider the private sector's role to help mitigate risks. Understanding the benefits and limits of private sector engagement will be critical, says Van Solinge. Much of the know-how and expertise resides with that sector.

> Emerging technologies have positively transformed how aid is delivered, but there are potential harms

Timo Koster, a consultant for the not-for-profit Domain Name Server (DNS) resolver Quad9 (a DNS resolver converts domain names into IP addresses), told *ISS Today* that 'this incident reiterates how important a multi-layer defence is against cyber-attacks.' Quad9, which has a large presence in sub-Saharan Africa, also has a real-time threat filter based on multiple intelligence feeds. It blocks access to malicious websites that spread malware or engage in stealing, defrauding and phishing.

As well as offering protection, the way such cyber security tools are distributed (e.g. to the humanitarian and non-governmental organisation (NGO) sector) and are populated by pooled threat information from the cyber security industry could become a model for the future. Central is the principle that the delivery of safe internet services should be considered a public good rather than simply a commercial proposition.

It's part of a wider debate about humanitarian aid and digital threats. In the real world the Red Cross has protections under international humanitarian law. The red cross or red crescent symbol is a potent globally recognised image of neutrality, and has a long history.

Over the past two years, the organisation has led a research project on the potential benefits and risks of a digital emblem. The purpose would be to flag the data and digital infrastructure of protected medical entities and certain humanitarian organisations and to signal their protection. However, one concern is that a form of digital branding could expose humanitarian data and assets to further attack by making it easier to target.

The Red Cross is under no illusion that a digital emblem would simply prevent cyber threats to the digital infrastructure of medical or humanitarian actors. Just as the physical emblem has never been a bullet-proof protection against physical attacks. However it is a way to signal legal protection and serve as a means of identification. It would allow cyber operators to more easily identify and spare protected entities in times of armed conflict, remind belligerents of their legal obligations where applicable, and deter other actors.

> The potential consequences of the contamination of humanitarian data are truly chilling

Organisations such as the Red Cross have played a key role at international policy level to entrench norms, including that stating that international law applies in cyberspace. It has applications not only for the use of the internet but also for other emerging tech areas, including drone technology and autonomous weapons, which also rely on networking capabilities.

Another area of focus is the possibility of establishing a dedicated 'cloud' for the humanitarian sector. So far research has been undertaken to consider the use of cloud technology for humanitarian supply chains. But a key requirement for secure cloud data storage for humanitarian purposes is that its integrity is maintained.

This is particularly critical given the Red Cross's function in re-uniting families in times of conflict. Imagine if data on unaccompanied children were hacked and data modified and people subsequently came forward pretending to be their parents? The potential consequences of data contamination are truly chilling, so humanitarian players must tread carefully.

As policy discussions on digital transformation across Africa gain more traction, international NGOs from the humanitarian world must note the potential risks and balance these against the benefits. Private sector expertise must be considered and speedy mitigation measures put in place.

Humanitarian players also need to continue to engage in multilateral discussions on cyber governance issues to ensure their needs are addressed.

Karen Allen, Consultant, ISS Pretoria

Exclusive rights to re-publish ISS Today articles have been given to Daily Maverick in South Africa and Premium Times in Nigeria. For media based outside South Africa and Nigeria that want to re-publish articles, or for queries about our re-publishing policy, email us.

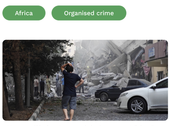
Photo: Rawpixel

Development partners

The ISS is grateful for support from the members of the ISS Partnership Forum: the Hanns Seidel Foundation, the European Union, the Open Society Foundations and the governments of Denmark, Ireland, the Netherlands, Norway and Sweden.

Related content

Africa | Organised crime



How will the Iran crisis impact Africa?

African refugees bear the brunt of shifting global politics

Africa can benefit from new global climate alliances

Foreign fishing vessels plunder Namibia's horse mackerel