Hacking the data of the world's most vulnerable is an outrage

By Robert Mardini, director-general, ICRC

The recent cyber-attack targeting humanitarian data belonging to 515,000 people was an affront to humanity, endangering those already suffering the effects of war or disaster.

They include people separated from their families due to conflict, migration and natural disaster, missing persons and their families, and people in detention. This data came from people all around the world, entrusting their private information to a humanitarian network whose help they desperately needed.

This is not a responsibility we have taken lightly. The ICRC has been long aware of the danger that our data could one day be the target of such an attack. We have implemented a range of enhancements in recent years due to the increasing threat of cyber-security attacks and worked with trusted partners to maintain high standards of data protection and systems.

But this attack shows that these systems are not immune to sophisticated cyber operations. And just as humanitarian workers should not be targeted by parties to a conflict, humanitarian data must also be respected and only used for humanitarian purposes.

A cyber-attack often means lost profits or exposed credit card details. In this case, this data could be potentially used to cause harm to extremely vulnerable people, including unaccompanied children. This attack is a violation of their privacy, safety and right to receive humanitarian protection and assistance.

The attack has also harmed our global network's ability to locate missing people and reconnect families. A topical example is the recent volcanic eruption and tsunami-induced flooding in the Pacific island nation of Tonga. Our work to help provide worried families and missing people with assistance has been hampered. So too has our tracing work in conflict areas, such as for Afghans fleeing violence.

Some 60 Red Cross or Red Crescent national societies now don't have access to the data they've contributed to this global system, so can't access case files on migrants fleeing conflict, disaster or extreme hunger. Thankfully, no data was deleted in the breach and we have teams working to set up interim systems that will allow us to continue this vital work.

What weighs heaviest on our hearts today is the risk of losing the trust of the people who need our help, privately and confidentially. We are finding ways to inform people whose data may have been accessed and explain the steps we're taking to protect their data in the future.

This incident is the latest in a worrying trend in which hospitals and humanitarian providers have been targets of cyber security attacks in recent years. Cyber-attacks have targeted medical facilities in places like the Czech Republic, France, Spain, Thailand, the United States and South Africa. These attacks may force surgeries to be postponed, and critical patients to be sent elsewhere. Attacks have delayed the processing of COVID-19 tests.

Collectively, we must hold the line: Cyber operations and attacks against medical entities and humanitarian data and organizations are dangerous, unacceptable and unlawful.

The Red Cross and Red Crescent Movement strives to be the best humanity has to offer. We help people in the worst of circumstances and uphold their dignity. This attack harms the vital work we all contribute to.

And to the people whose data has been hacked: we know you entrusted us with personal information and details about traumatic events in your lives. We want you to know we are doing everything we can to restore the services that we offer across the world. We will work hard to maintain your trust so we can continue to serve you.