



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

6.3 Cyber Ops against humanitarian organizations - ITW with Felipe

Concepts (extracted from automatically generated subtitles):

Cyber operations. Growing risks. Humanitarian organisations. Data breaches. Felipe ramirez mock-kow. Potential risk. Potential impacts of cyber operations. Red crescent movement. Red cross. Civil society organisations. Potential risks. Icrc colleague. Examples of cyber operations. Day-to-day work of a movement. Different countries.



[to video sequence search](#)

(within Understanding the digital supply chain and its stakes for humanitarian actors.)



[to video](#)

Center for Digital Education. More educational support material here:

<https://www.epfl.ch/education/educational-initiatives/cede/educational-technologies-gallery/boocs-en/>

page 1/69



Cyber operations against humanitarian organizations

Cléa Thouin interviewing Felipe Ramirez Mokkow

Protection in the Digital Age specialist, ICRC
Head of Protection of Family Links Unit, ICRC



...

notes

summary

0m 0s



Welcome



Welcome back. In this video, we'll be looking at cyber operations against humanitarian organisations

notes

summary

0m 4s



Welcome



and their impact not only on the organisations themselves, but on the people that they aim to assist and protect. Cyber operations against humanitarian and civil society organisations

notes

summary

0m 13s



Welcome



have become more and more common. In 2023, for example, the UN alone reported a 170% increase in malicious cyber activities against it compared to 2022.

notes

summary

0m 25s



Welcome



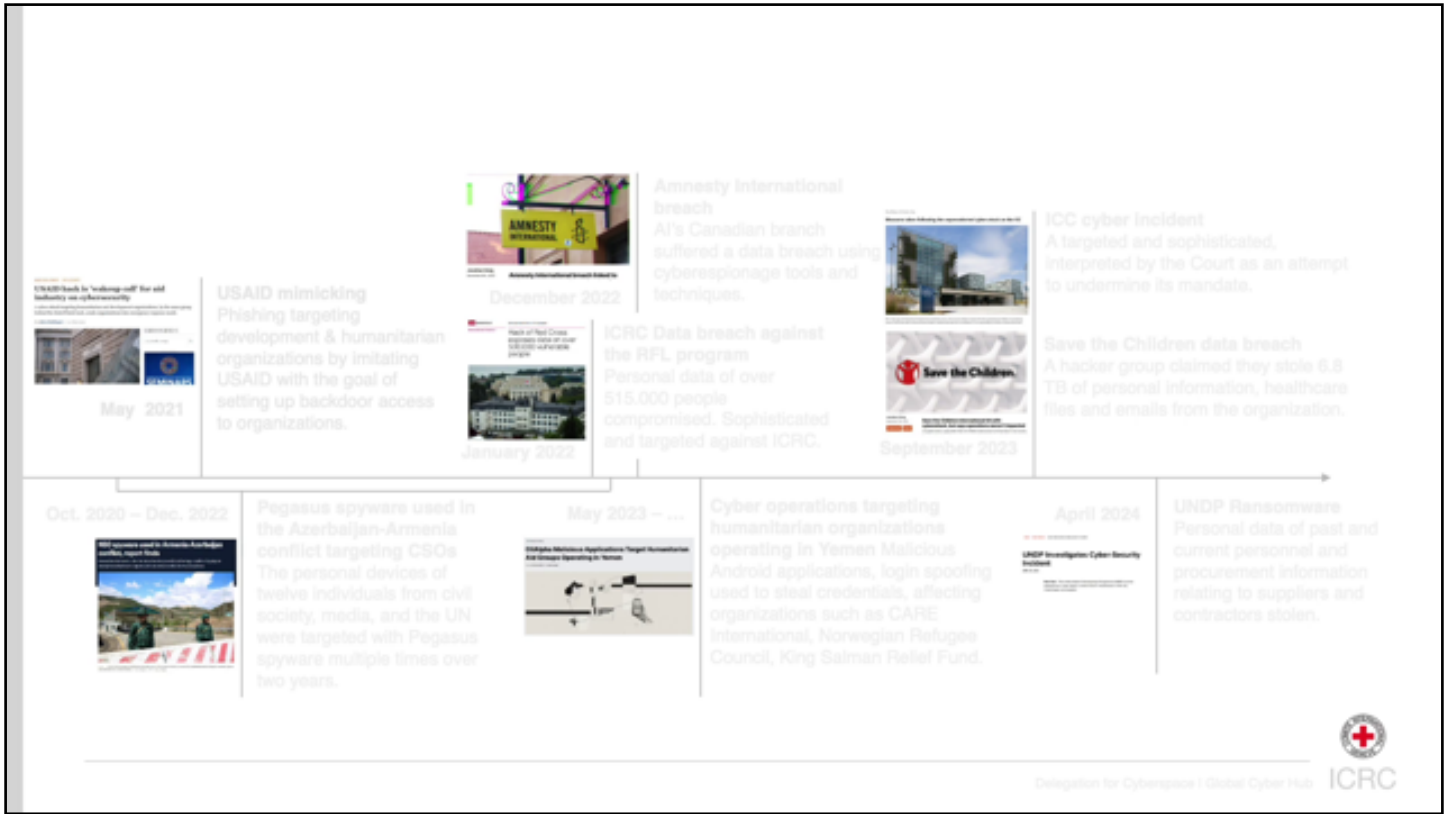
Similarly, in a survey of its NGO members, the organisation NetHope saw an increase in the number of members that experienced a cyber incident from 45% in 2022 to 65% in 2023.

notes

summary

0m 37s





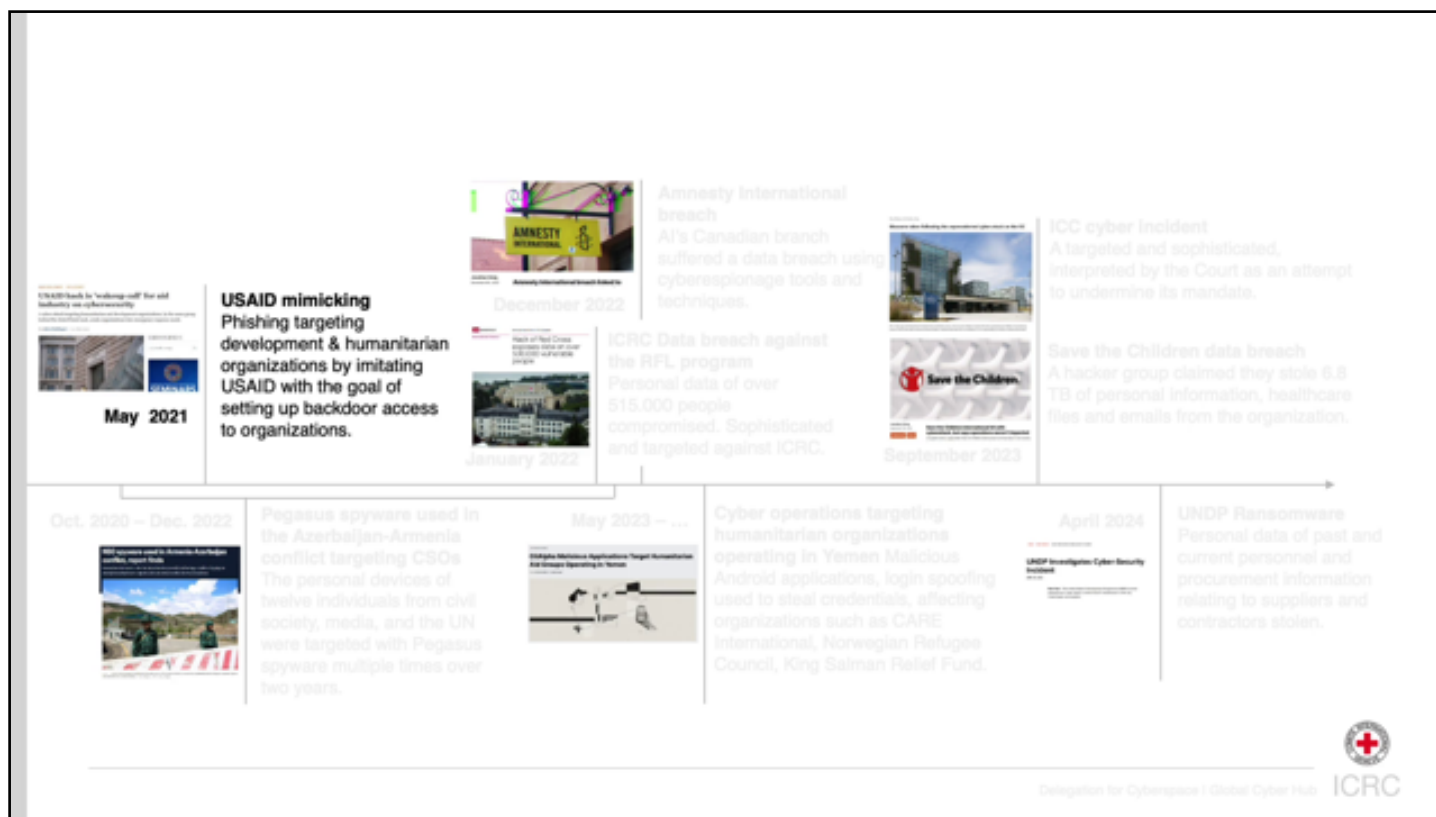
There aren't many publicly documented examples of cyber operations against humanitarian organisations, but the few that have been reported on, illustrate the growing risks faced by the sector.

notes

summary

0m 53s





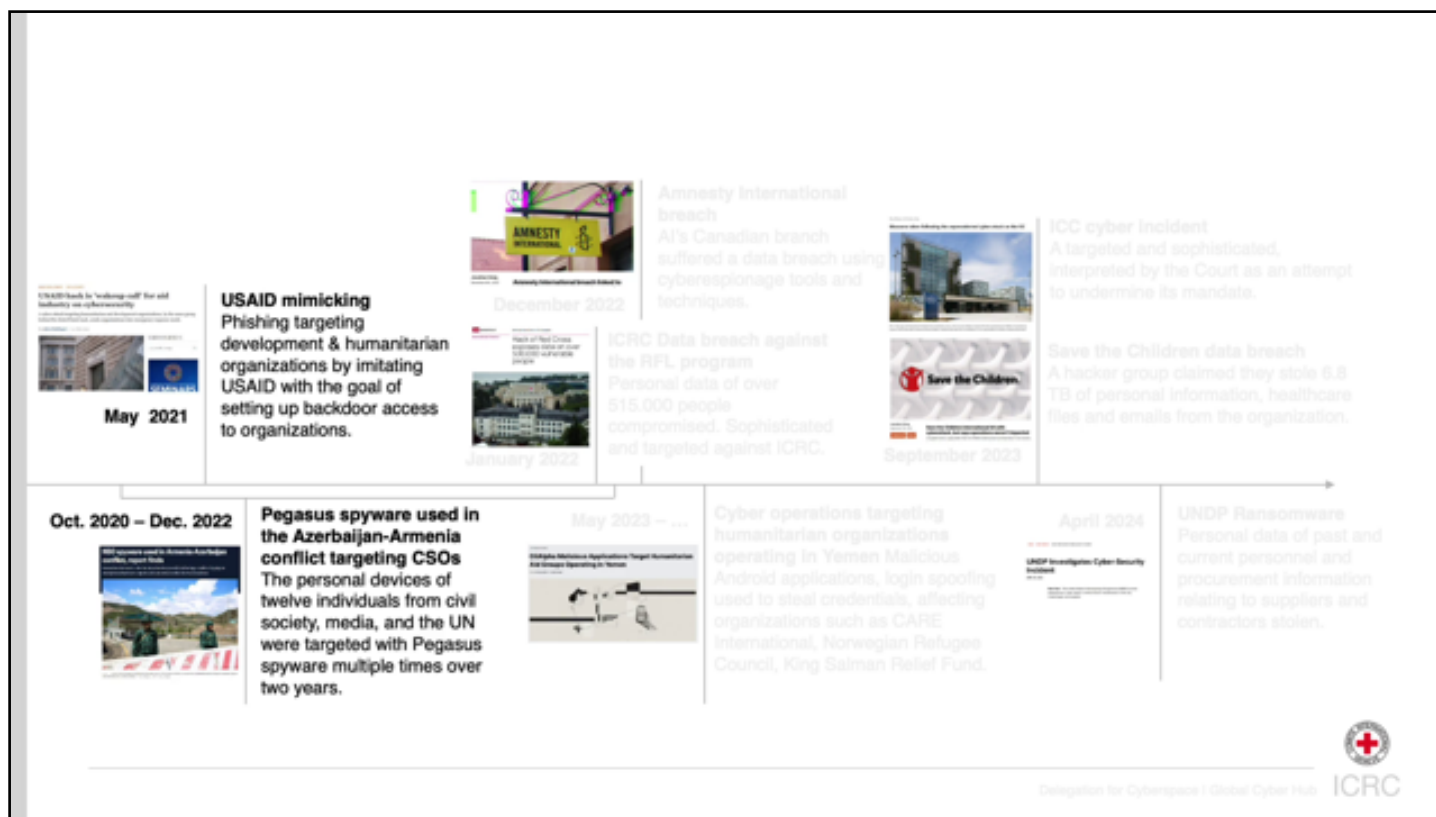
Some examples include a 2021 phishing campaign, impersonating USAID,

notes

summary

1m 8s





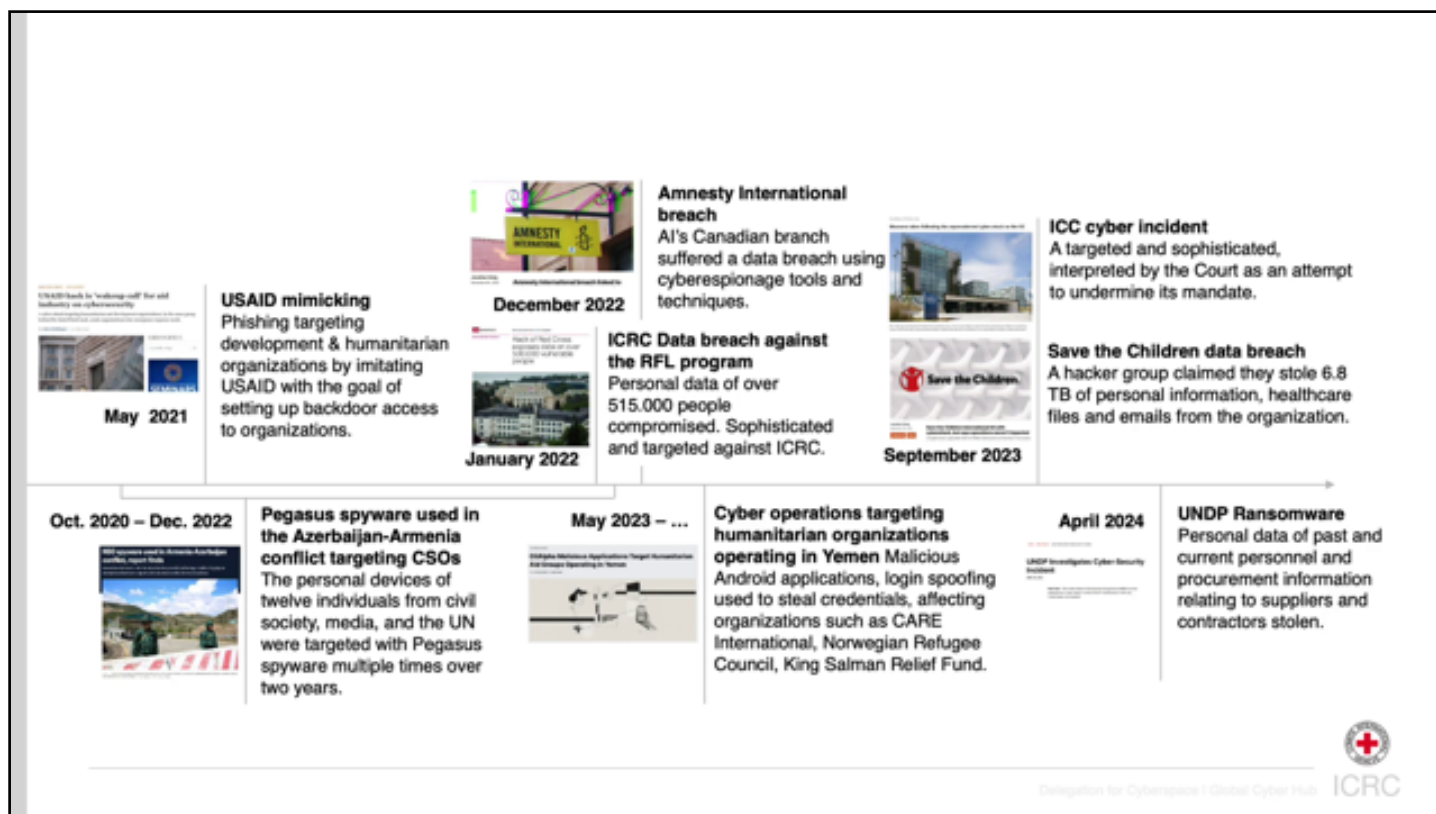
that targeted over 150 NGOs aiming to compromise beneficiary and staff information. From 2020 to 2022,

notes

summary

1m 14s





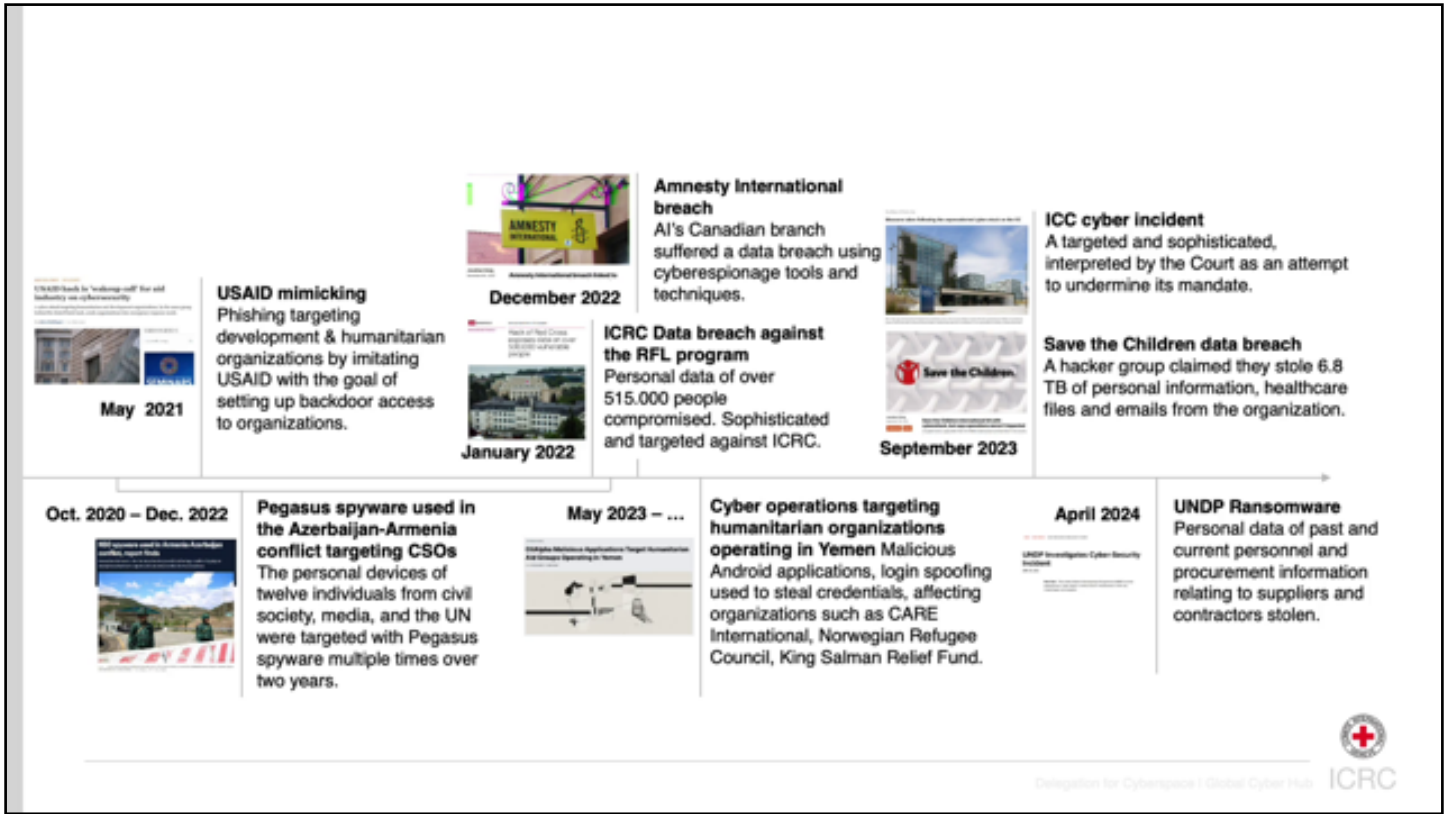
the Pegasus spyware was reportedly used to monitor civil society, the UN, and media organisations during the Azerbaijan-Armenia conflict.

notes

summary

1m 25s





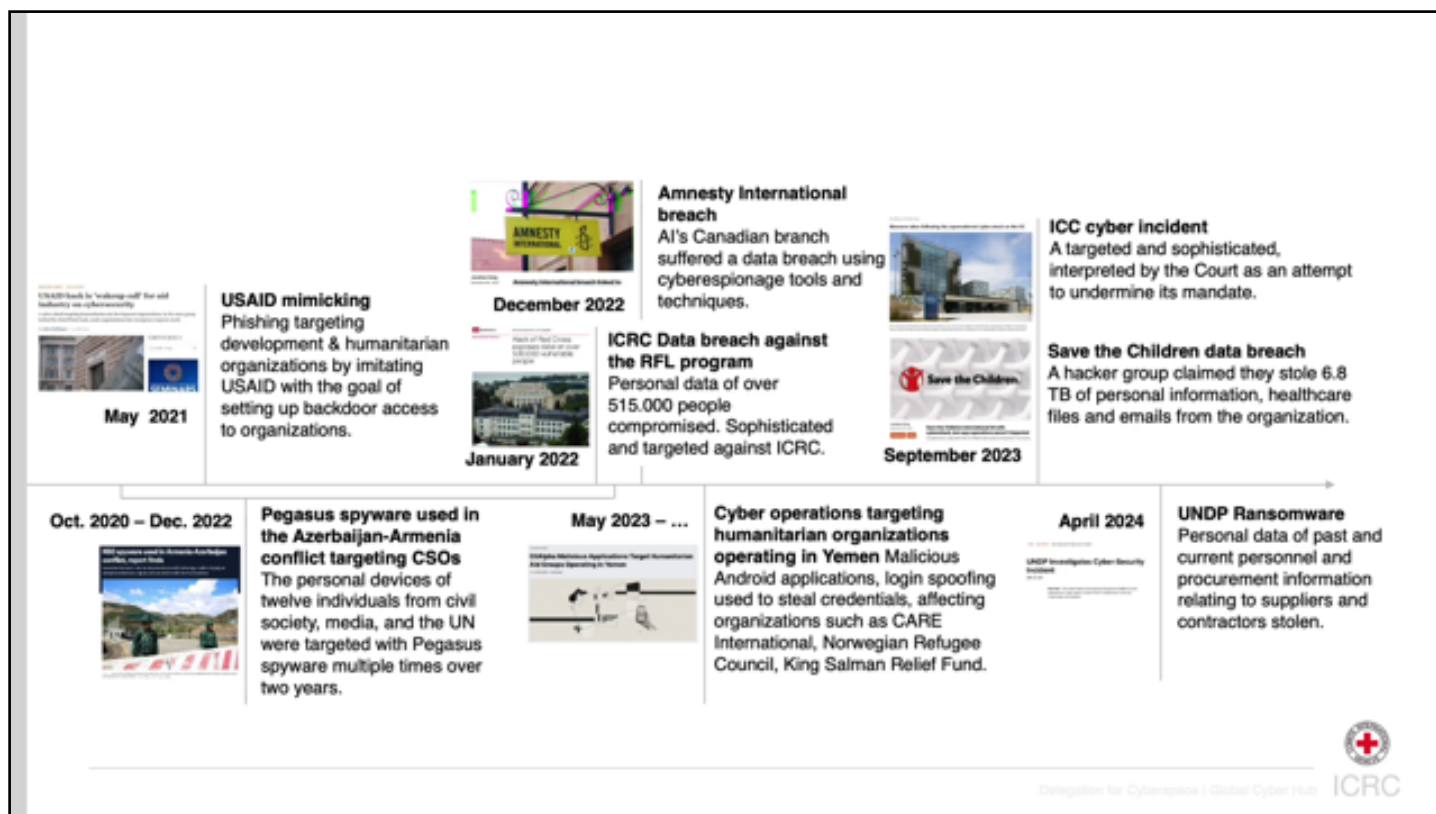
More recently, several cyber operations have reportedly led to data breaches,

notes

summary

1m 37s





including against the ICRC in 2022, which we'll talk more about today, but also against Save the Children International in 2023 and the UNDP in 2024.

notes

summary

1m 44s



Cyber Operations against Humanitarian Organizations



The consequences of such cyber operations have been varied, and in many cases, their full extent remains to be determined.

notes

summary

1m 54s



Cyber Operations against Humanitarian Organizations



But it's important to understand that because humanitarian actors often hold sensitive personal data, cyber operations can have severe implications for the people the data belongs to.

notes

summary

2m 1s



Cyber Operations against Humanitarian Organizations



Implications such as detention, persecution, physical injury, or even death. People may experience such harm

notes

summary

2m 13s



Cyber Operations against Humanitarian Organizations



months or even years after the initial operation, and it may be very difficult to establish a causal link between the harm and the cyber operation. To illustrate the potential impacts

notes

summary

2m 25s



Cyber Operations against Humanitarian Organizations



of cyber operations against humanitarian organisations, we're joined by my ICRC colleague, Felipe Ramirez Mock-Kow. Felipe is the Head of the Protection of Family Links Unit at the ICRC's Central Tracing Agency.

notes

summary

2m 37s



Cyber Operations against Humanitarian Organizations



He's been with the ICRC since 2012, and with the Central Tracing Agency since 2022, where among many other responsibilities,

notes

summary

2m 49s





he works with a team of specialists that respond to data breaches affecting the Red Cross and Red Crescent movement. Felipe, it's great to have you with us today. Thank you so much for the invitation. I'm very happy to be here with you.

notes

summary

3m 1s



ICRC data breach - Why is the ICRC collecting data?

Interview with Felipe Ramirez Morkow



Felipe, in January 2022, the ICRC discovered

notes

summary

3m 13s



ICRC data breach - Why is the ICRC collecting data?

Interview with Felipe Ramirez Molkow



that servers hosting personal data belonging to more than 500,000 people receiving services from the International Red Cross and Red Crescent Movement had been breached. I'd like to ask you some questions about the impact of this breach. But first, could you explain to us in a few words

notes

summary

3m 16s



ICRC data breach - Why is the ICRC collecting data?

Interview with Felipe Ramirez Molkow



why the ICRC is even collecting this personal data?

notes

summary

3m 36s





Of course. In situations of armed conflict and other humanitarian emergencies, the Red Cross and Red Crescent Movement, which includes, of course,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

3m 40s





the International Committee of the Red Cross, we work together to reconnect separated families and to search for missing persons. This is what we call Restoring Family Link services or RFL services.

notes

summary

3m 49s





To do so, it would be impossible to achieve any results without collecting and using personal data.

notes

summary

4m 6s





Just to give you an example, if we are looking for a missing person, we would need to know who this person is, what is his or her name, where they were born, their age, et cetera,

notes

summary

4m 13s



Operational Impact of the Breach



in order to achieve a result, to search, and to provide an answer to their families. Thanks for that explanation. Very practically, what was the impact of a breach on the day-to-day work of a movement?

notes

summary

4m 25s





What did this mean for people using their services? Well, the most significant impact was the disruption of the operational continuity

notes

summary

4m 37s





of the movement's RFL service, the movement RFL's work. As soon as the breach was discovered, what the ICRC did is took down the compromised servers, so they went offline,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....





which prevented any further incidents to happen, but it also hinder our capacity and the capacity of the Red Cross and Red Crescent national societies around the world to continue providing RFL services.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

5m 1s





Of course, a number of measures were taken to improve the security, and the systems were restored only when we had checked and tested that it was safe

notes

summary

5m 13s





for us to continue using those servers. But given the scale of the incident, and here we're talking about 500,000 persons

notes

summary

5m 25s





that were concerned their data was concerned by this incident, all of the resources that are normally dedicated to carrying out RFL work, meaning providing contacts for separated families or searching for missing persons,

notes

summary

5m 37s





were instead invested in responding to this incident, to analyse the compromised data, to assess the potential risk and impact of the breach,

notes

summary

5m 49s





to notify impacted individuals, often that was done in person. Of course, this was extremely resource-intensive, and therefore, all of our services around the world were hindered by it.

notes

summary

6m 1s





Some components of the movement, to be quite honest, had it even worse because they completely put their services on hold. Others did it only partially.

notes

summary

6m 13s





But at the end of the day, what happened is that we were not able to open any new cases for separated families. We were not able to provide updates to the families on the existing cases that we already had.

notes

summary

6m 25s





Of course, we were not able to conduct searches for missing persons. The impact varied, of course, as I mentioned already throughout the movement and throughout the world and depending on the context.

notes

summary

6m 37s





But this is because the movement is an interconnected network, and the RFL service is often a transnational effort of all of us together. The impact on some parts reverberated throughout the entire network.

notes

summary

6m 49s





That sounds like quite a significant impact. How long did it last? Well, actually, I can tell you that we can still feel the impact of the breach today, 2 years later.

notes

summary

7m 1s





Normal activities resume within a few months, but the breach has still long-lasting impact, both in terms of the tools that we use as a movement altogether to carry out these activities,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

7m 13s





but also in terms of the staff and the perception of the service itself. On the one side, our staff, the RFL staff throughout the movement,

notes

summary

7m 25s





builds a relationship of trust with the people they collect that information from in order to act on their behalf and upon their request.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

7m 37s



.....

.....

.....

.....

.....



These breaches have an impact on the trust that we are able to build and sustain with the people we are working with. It leads to a loss of trust, and it does by default,

notes

summary

7m 49s





it affects the entire movement's ability to continue providing this service efficiently. On the other side, we were also very much concerned

notes

summary

8m 1s





about the potential risks these data breaches could have on the people whose data was exposed. To maintain, and in some cases, rebuild this trust,

notes

summary

8m 13s





taking, of course, into consideration the risks that we had identified, we had to make sure that communication was done in an open and transparent way with those families that were affected.

notes

summary

8m 25s





We had to accompany them. We had to answer the questions. We had to take into consideration their concerns. We needed to make sure that if there was ever a risk

notes

summary

8m 37s



Potential Risks for Affected Individuals



that materialised, we were there. We were there with them, and we were there to support them. This, of course, takes a lot of resources. It takes a lot of time, and we continue to see it to this day.

notes

summary

8m 49s





Let's talk more about that. What were some of the potential risks that the ICRC identified for the people whose data was breached? I would say that the most significant challenge

notes

summary

9m 1s





that we faced was the uncertainty that surrounded and continues to surround the breach. Because while we knew that the system had been compromised,

notes

summary

9m 13s





that there was a breach of our data, we couldn't really confirm if the data was extracted, and if it was, how it would be used or how it could be used.

notes

summary

9m 25s





For us, it was... Although we were able to identify that the data was not tampered, nothing was really changed, we cannot rule out the possibility that it was copied and that it was exported.

notes

summary

9m 37s





Therefore, we didn't know how it could be used later. To this day, however, we know, and we are sure that there is no evidence that the data has been used,

notes

summary

9m 49s





has been leaked anywhere. That part is important to be remembered. Now, because of all of this uncertainty

notes

summary

10m 1s





and because of all of these possibilities and risks that we identified, we decided to adopt the most protective approach. That means that we work under the assumption that all of the data was extracted and all of the data could be misused.

notes

summary

10m 13s





With that in mind, what we did was to identify a range of risks for the affected persons. Those risks we share with the rest of the components of the movement,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

10m 25s



.....

.....

.....

.....

.....



the Red Cross, Red Crescent movement, for them to contextualise them, for them to understand how these risks would apply in their different countries, in the different contexts because of the different dynamics they deal with.

notes

summary

10m 37s





This risk, among others, include the risk of fraud, identity theft, retaliation, extortion,

notes

summary

10m 49s





even the impersonation of the movement staff, for example. The most difficult part, I guess, is to assess really what is the likelihood

notes

summary

11m 3s





of this risk actually materialising, actually occurring in a specific location, and to measure what is the potential impact of that risk materialising.

notes

summary

11m 13s





Another difficulty is in case it does materialise at this stage,

notes

summary

11m 25s





how to establish the causal link to the breach itself. This part will not be easy.

notes

summary

11m 33s





Very interesting. Thanks for sharing that perspective. Especially how challenging it can be to identify some of the risks. What did the ICRC learn from this experience? We learned a lot.

notes

summary

11m 37s





We learned that no organisation is immune to the risk of cyber operations, and that this reality is something that we have to take into account

notes

summary

11m 49s





in our current operations and include in our contingency plans to be better prepared, to be honest. It really helped us identify the different vulnerabilities

notes

summary

12m 1s





on the different gaps that we might have in our practices and in our processes that we were able to address in order to strengthen our defences and in order to strengthen our plans to respond better

notes

summary

12m 13s





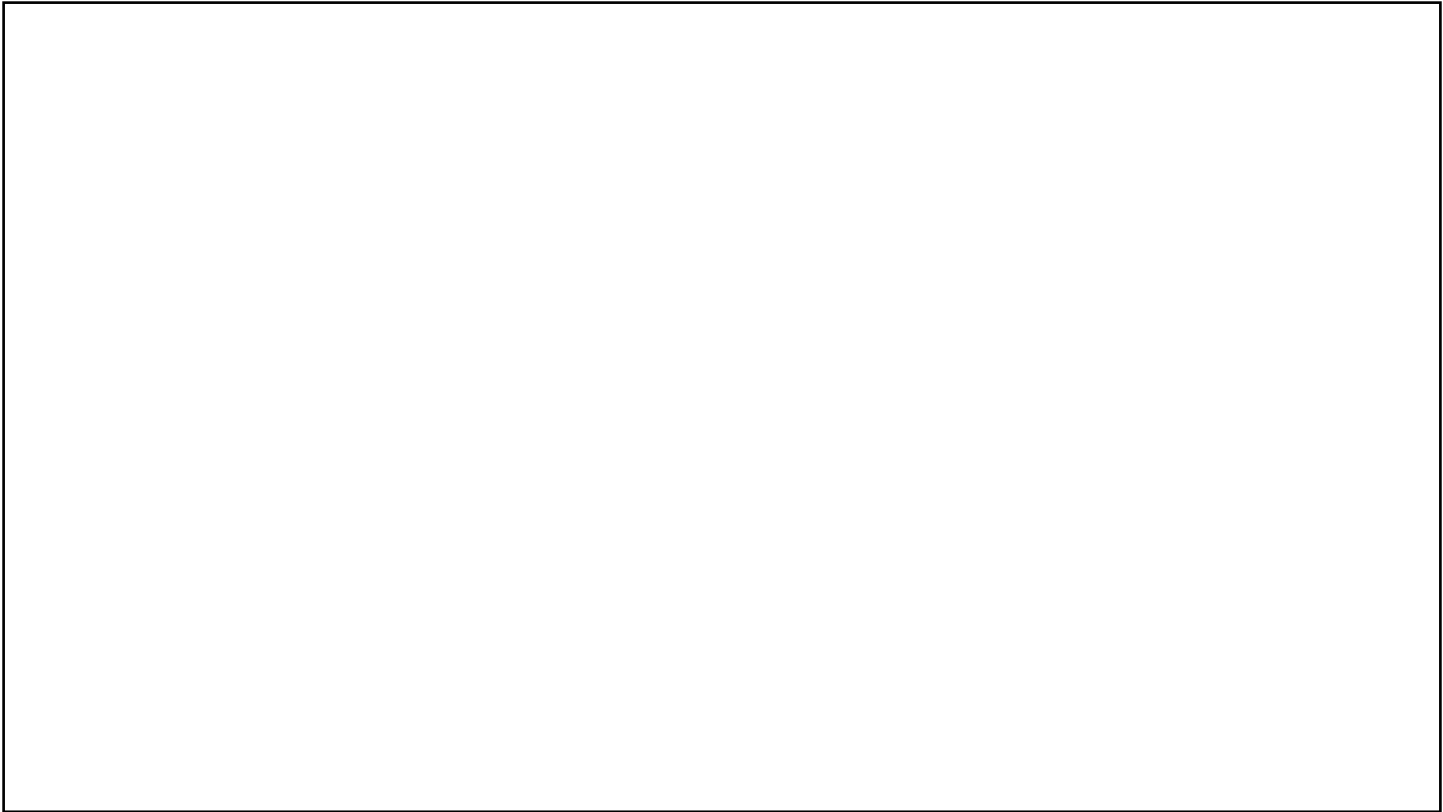
in case anything like this happens again. Of course, it really helped us identifying the risks

notes

summary

12m 25s





and the mitigation measures that we could immediately put into place if this ever happens again. Felipe, thanks so much for talking to us today and helping us better understand the potential real-life impact of cyber operations. Thank you very much for having me. It was a pleasure. Have a very nice day.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

12m 37s



.....

.....

.....

.....

.....