Just to give you an idea of how something like this would go from my end:

1) Setup a website, domain, etc. - you want to setup a website of course. There are a few ways I can make the site and we can talk about that, but likely the best way to begin will be using a basic blog-like system with an encrypted messaging (private) section so that you can easily access and update the site instead of working with raw code. From there we can move on to more complex methods.

2) Secure the website - this is one of my passions, cryptography. I think it is very important for this kind of project as well. So firstly I don't use shared hosting for any projects: I use servers that I have access to from the root level so that I can implement security procedures. Basic security like HTTPS (what you see with any bank or PayPal, etc.) of course, but also more advanced security rules to prevent any type of hacking on the server side. These are updated every month or two depending on when the core libraries are updated; I keep watch for these all the time.

3) Tor service as a start - I am sure you are familiar with Tor; so we can setup very easily a Tor URL hidden service which will be a mirror of your site but hosted on Tor so that anyone who wishes to use Tor to access the website can do so without divulging their IP address. Again, it is a mirror of the website so any changes made to the main site will be pushed to the Tor site - it is just a security precaution for people in sensitive countries. Very simple to do.

4) Default encryption and optional end-to-end (E2E) encryption for private messages and a messaging system for contacting which I have built before and can build in quite easily - what I mean is a secure way for someone to contact you or the organization. I am not sure if you are familiar with PGP, but it is the standard for basic encrypted end-to-end messages where no one can view them but the receiver and sender..however it requires a knowledge of setting up PGP which isn't hard, but not automatic.

So I can put a guide up on the site for people who want to take the extra step. Also just a general guide on security for people who want to message from sensitive countries.

However as principle when I make a site I want to make it as easy as I can for the basic user so:

- by *default* any messages sent will be encrypted with the server PGP key, that is they'll be encrypted automatically with a PGP key that is securely stored on the web server itself and then sent, and when you or anyone with access reads them they'll be decrypted based on the fact that you or anyone who has access has the decryption key (automatically) attached to their login.

This makes it easy for someone who isn't technical and doesn't want to use PGP themselves, so they can type normally and send a message but that message is encrypted using PGP automatically using the website's key stored on the server (so the website is acting like the middle-man and encrypting the message for the user without them seeing the technicalities) and thus making it secure for them. From a super theoretical point of view, it is not AS secure as someone using their own PGP key and then you decrypting it on your end, because you are trusting the website to be secure i.e. you are trusting that whoever controls the website isn't someone malicious like the government, but it doesn't matter as

much in this case. It matters more if you are, for example, buying something from the darkness that is not legal and you are trusting the darknet website to encrypt for you; you don't know who's in control there so that's where something like this matters more.

5) Secure Access for Administrators like you - from the standpoint of the site, it'll be as secure as it can get to modern standards. I follow encryption daily and the most advanced mechanisms are employed on the server end.

The only way someone can "hack" the site is if someone can get your/an admins password through some malware or whatnot, classic hacking. There are many ways to prevent this: basic security for your personal use, ensuring your computer has no viruses, using Tor to login as a stopgap just because that allows for basic IP security.

Also more advanced ways - not sure if you are familiar with Tails but it is a Linux-based operating system that is extremely secure by default and only allows access to the internet via. very secure means..this is the extreme end of the spectrum where you login only through Tails but this probably isn't required unless this becomes big, but I like to mention it because I am security oriented.

6) Legal setup of the organization — want to get the organization legally registered, which involves two things: the first one is pretty fast/easy which is getting your nonprofit registered at the state level. Most states offer online registration but even if they don't it's very simple, this takes a few days to process depending on the state and then you have a nonprofit organization that is recognized by the state. Your nonprofit will show up in the state database and you will have an EIN (like a social security number for businesses) that can be used for donations, but:

The other more important part after the state is the IRS (federal), where you get your 501c registration status - that is nonprofit organization for taxation by the IRS for donations. Two benefits of course:

<u>One</u> is that you are tax-exempt for any donations;

<u>Two</u> is that wealthy people are more inclined to actually donate to a IRS-recognized 501(c)-type organization because they can *legally* write off any donations on their tax returns. Key word being legal for them to do so. Just how the system works, lol.

This takes a few weeks as the IRS does some basic "verification" to make sure you aren't cheating into non-profit, however it's nothing advanced — just need to have clear mission statement, etc. and I can help you with all of that.

Once all of that is done, we can go from there.

** **One thing I do NOT have experience with** is the actual method of visa applications and getting people safely out of the country. That is where I think as the organization grows you can get people to assist with this; I believe people like Faisal Saeed AlMutar have experience with this and it's the riskier process.

** One ***BENEFIT*** of all this is that unlike the other nonprofit I helped setup for a friend of mine which was about civil liberties in the US/Patriot Act etc. — this one isn't "going against" any Untied States interests, that is there is no worry that the US Government will want access to any of this because we aren't doing anything that is questionable whatsoever. And we are not harboring any type of illegal activity at all. So all encrypted messages, etc. will not be of worry. And the organization is based in the US, so we are not under any jurisdiction of laws from Saudi Arabia or any Middle Eastern nation or any nation that isn't the United States — so we do not have to worry about Saudi Arabia trying to issue any of their laws against the site and the organization is governed by US laws, which makes this all completely legal and safe for us - of course as mentioned the people sending messages will have to do so securely but I will do everything I can to ensure that this happens both automatically and, if the user wishes, with extra ("true") end to end encryption for extra security.