The Guardians of GOOD WORK

The most vulnerable organizations may not understand their exposure to online attackers.

CEO **STÉPHANE DUGUIN** tells Brunswick's **MARK SEIFERT** how CyberPeace is building NGO defenses.

Stéphane Duguin has spent decades studying how criminals and terrorist groups weaponize technology against vulnerable communities. He is the CEO of the CyberPeace Institute, which provides free cybersecurity for the most vulnerable—often organizations that don't even recognize their exposure to such threats. The institute also investigates and works for accountability for threat actors.

Duguin is a member of several international bodies involved in cybersecurity, including the Incubation Advisory Board of the Open Quantum Institute and the Global Forum on Cyber Expertise. He sees his organization as building not just case-by-case resolutions, but systemic change, toward what he calls a culture of Cyber Peace.

As co-Chair of Brunswick's global Cybersecurity, Data & Privacy practice, Mark Seifert helps clients prepare for cybersecurity incidents—and respond to them. Seifert attended the Munich Cybersecurity Conference conference this year, where he was impressed by Duguin's presentation.

Back at Brunswick's office in Washington, he spoke with Duguin on video at his office in Geneva. Duguin explained how the Institute offers tech professionals and companies in the for-profit world a way of giving back that could help bring peace to the online world.

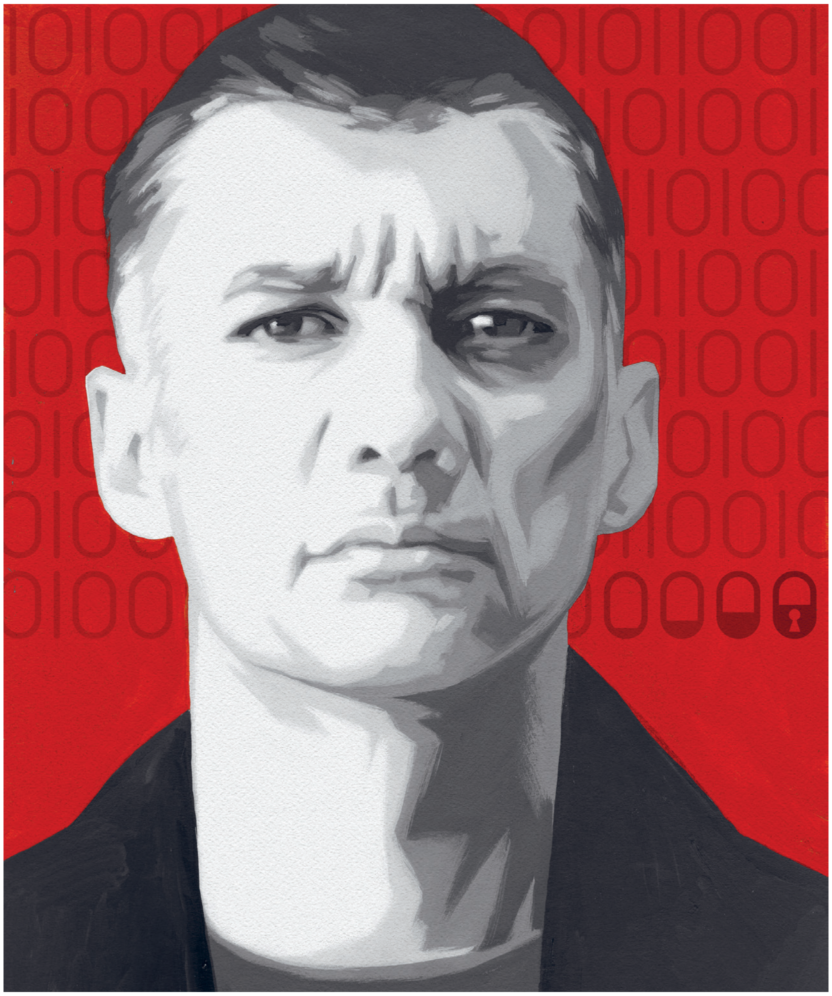

ILLUSTRATION: THOMAS FUCHS

Tell us your background, how did you get here?
I was working for Europol in The Hague when I was asked if I wanted to help set up the CyberPeace Institute, and I started in December 2019. Behind the project, providing seed funding for what became the CyberPeace Institute, were the Mastercard Center for Inclusive Growth, the Hewlett Foundation, Microsoft and the Ford Foundation.

Five years down the line, our headquarters is in Geneva, we've opened an office in The Hague in the Netherlands and we have about 30 employees.

Do those employees primarily connect an NGO seeking help with a cyber advisor? Or do you also provide advisory services?
We have in-house cybersecurity experts who can provide cybersecurity work for NGOs from technical support right up to policy advice. We started the

program of free cybersecurity for NGOs globally. We piloted it in Switzerland because that's where we were, and now we have this program where we provide support to more than 500 NGOs globally.

In the US, we had the support and partnership of the Craig Newmark Philanthropies, and we work with the Center for Long-term Cybersecurity at UC Berkeley to deploy their network of volunteers everywhere in the US to provide cyber volunteering for critical infrastructure, underserved communities, K12 entities, schools, healthcare. That's an ongoing program. It's called the Cyber Resilience Corps.

There's a full ecosystem of NGOs and nonprofits in the US, which is absolutely underserved in cybersecurity. In some states, the smaller ones are undersourced and we are working now on a program to provide free actionable volunteer capabilities to these entities.

And that's the wealthiest nation in the world. What are the exposures in Malaysia or Brazil?

The mandate I was given was to look into systemic solutions for the most vulnerable in cyberspace. If you really go down that line, any organization that is connected to the internet is vulnerable.

But clearly, a small nonprofit NGO lacks the resources to protect itself. So that's why we decided to focus on NGOs, because we discovered that this sector—NGOs, nonprofits—are under-resourced when it comes to IT and cybersecurity. At the same time, NGOs are a sector that is attacked by everyone—criminals, state actors, activists.

There was an urgent need, and no one was really looking into it. Cybersecurity companies aren't interested because NGOs can't afford them. Nation states are absolutely not supporting NGOs when it comes to cybersecurity.

When you support NGOs, you end up supporting access to health, access to food, shelter, aid, development, humanitarian and relief support, the fight against gender-based violence and the fight against climate change.

We identified some funders that were interested in safeguarding the cybersecurity of NGOs in the climate change fight—and we are looking for funding for other sectors of NGOs.

So perhaps the ideal would be to persuade a major oil company who is concerned about climate change to support your work with climate-change NGOs?

When we started this NGO-supporting program, the comment that we heard from a lot of NGOs was, "I do not want to be supported by companies that are not aligned with our mission."

It was excellent feedback and we engineered our matchmaking platform having that in mind. We have more than 1,500 volunteers now, but we can filter who is going to help whom. That's quite important and it works both ways. We have companies telling us they will never support a certain type of NGO.

How do you find volunteers?

There is a huge talent shortage. There is not enough cybersecurity talent on the planet to face the problem that we're having. And for sure, NGOs are not a priority for the talent that's out there. So the CyberPeace Institute seeks talent in big companies, where we find that many cybersecurity experts have their heart in the right place, and want to help defend the defenseless.

When you offer the chief information security officer at a big company the opportunity for their team to help Doctors Without Borders or Save the Children, I don't even have to finish the sentence.

> "WHEN YOU OFFER THE CHIEF INFORMATION SECURITY OFFICER AT A BIG COMPANY THE OPPORTUNITY FOR THEIR TEAM TO HELP DOCTORS WITHOUT BORDERS OR SAVE THE CHILDREN, I DON'T EVEN HAVE TO FINISH THE SENTENCE."

Are you seeing geographically concentrated attacks on NGOs or are the attacks more sector or subject-matter based? Help me to understand where you're seeing hot spots of trouble.

Healthcare is always a hot spot, and NGOs generally have become a hot spot. But geographically, the numbers we have are skewed. We have the numbers where we have the reporting.

In the first data collection that we did, there was an over-representation of NGOs in the US which were under cyberattack. Why? Because there is more stringent reporting from these NGOs because of their funding mechanism, which requires them to report a problem. In other parts of the world, if you don't have this reporting requirement in your funding mechanism or in your governance model, then NGOs are under attack and the public may never know.

If I'm hearing you correctly, one of your pieces of policy advice to funders would be, "Make your grant recipients report cybersecurity issues so that we can help make them more safe."

Exactly.

At the same time, I wonder why they wouldn't report, even without that requirement?

You'd think it would have been straightforward to get NGOs to take advantage of our programs. You offer free cybersecurity, NGOs are going to jump in, right?

Not so fast. The first question was always, "Why me? I'm an NGO. I'm not under attack. What are you talking about?" The notion of a cyberattack is not even very clear to them.

Or maybe they'd seen it happen at another NGO, and that NGO had lost funding as a result of reporting the attack. Because they were public about it, funders told them, "You're not really stringent with the money that I'm giving you so next time forget about me as a source."

That's why we started this program not by looking into the reporting but by offering free cybersecurity. We bring you through a baseline assessment of where you are, the support you need and then we offer it at the level you need.

We deploy a volunteer, short term, to move the NGO up the ladder of cyber-maturity. It's gradual, but it's always aimed at cybersecurity maturity. After we create this community of trust, we start talking about reporting. Then we say, "You know what's happening to you? It's important to share because it can help the others." But we don't start with that concept—we bring them along.

What's the most common threat you're seeing with NGOs these days? Is it ransomware? Data theft? Spyware? The whole range?

The attacks against NGOs are comparable to the attacks you see impacting other small and medium-sized enterprises. NGOs can be vulnerable to big, undiscriminated attacks because of systems that are not patched or badly installed. There's a lot of phishing. And indirect victimization resulting from credential stealing and credential selling.

We also see a large number of attacks tied to geopolitics, among which is the employment of spyware against nonprofits. As soon as there's a geopolitical context, the attacker uses everything they have against their targets. We saw that with nonprofits in Ukraine, for example. They were targeted by campaigns of disinformation to break the trust between them and society. And at the same time, they were targeted by cyberattacks, some of them disruptive enough to destroy the system, and some of them used very insidious means to steal their data.

How do you balance day-to-day duties with an urgent and demanding situation like Ukraine?

A few weeks after the Russian invasion, we put in place the "CyberPeace Institute: Cybersecurity In Times of Conflict #UKRAINE" platform where we track and trace cyberattacks and disinformation targeting civilians since the invasion of Ukraine.

"THE FIRST QUESTION WAS ALWAYS, 'WHY ME? I'M AN NGO. I'M NOT UNDER ATTACK. WHAT ARE YOU TALKING ABOUT?' THE NOTION OF A CYBERATTACK IS NOT EVEN VERY CLEAR TO THEM."

We could only sustain this platform until the end of 2023 because of funding. As you know, there are budget cuts everywhere. So now we have the platform, but it's dry on data because we just don't have the capacity, to your point, to continue with this specific program.

If I am reading this and I'm on the board of an NGO, how can my NGO take advantage of the services you offer?

If you are on the board of an NGO, advise your CEO to sign onto our NGO CEO Call to Action letter to governments around the world. You can also ask your executive team to join the CyberPeace Builders to provide cybersecurity support. Executive-level support helps gain the benefit of donors. On the technical level, it doesn't have to be a cyber expert. It has to be someone in the organization who really wants the organization to be defending against the threat. Sometimes that person is a communications officer who doubles as an IT expert 20% of the time.

As soon as we are contacted by these people, we put them through a very light cybersecurity assessment in order to get a baseline. And from that baseline, we have the capacity to deploy a few hours of technical help right away. If you need some training on phishing, I can deploy to you right away two or three hours of phishing training from one of our 1,500 volunteers.

We have a valuable partnership with Cloudflare that allows us to deploy an email security quarantine program pro bono to help NGOs intercept cyberattacks. Currently, more than 25 NGOs are leveraging this program. Over 200,000 emails have been successfully quarantined, and we have blocked numerous campaigns targeting specific funding aspects of these NGOs. These alerts have enabled us to share potential threats with the entire community, helping to block them effectively.

On the threat intelligence front, in collaboration with our partners Bitsight, Kaduu, Microsoft and Dataminr, we have identified over 700 infections among our beneficiaries. We have issued more than 549 alerts about real incidents and resolved them. Additionally, we have monitored over 800 vulnerabilities across more than 300 organizations and provided them with guidance on how to mitigate these risks. Our proactive approach ensures that these organizations are well-informed and can take necessary actions to protect themselves.

A word of advice for NGOs about AI. We see a lot of nonprofits deploying AI just because everyone is telling them that they need to. But let's not create new vulnerabilities and new exposure because of badly implemented AI strategy. The CyberPeace Institute is advising our partner NGOs about how to implement AI in a more secure way.

If my company does something—say, it manufactures shoes—that bears no obvious level of expertise that could help your work but we support your goals, what are the different ways that we can help your mission?

We have a standard partnership with any and every sector to support the CyberPeace Builders program. One is a program of cyber volunteers. The volunteer doesn't have to be a cybersecurity expert. We have data protection officers, IT engineers. We have a network made up of a lot of different profiles. So on one end is your workforce.

On the other end, any company can contribute funding. Normally the partnerships that we have average $25,000 yearly. That $25,000 and those volunteers have a direct impact on protecting NGOs supported by the CyberPeace Institute.

For companies that provide volunteers or funding or both, we provide you a scorecard about how your money and time has been used. Joining this program allows you to support a global action plan, the Beyond 125 Action Plan, launched in The Hague at the Peace Palace.

This initiative aims to provide 10,000 NGOs with free cybersecurity assistance and AI solutions by 2026. It's an ambitious effort to drive global action in protecting underfunded civil society organizations against cyber threats and disinformation. We show you exactly how you are supporting so many NGOs across so many sectors.

So far, the majority of these partners joining us are not from cybersecurity companies. There are some from tech and a lot from finance. We also have support from the retail sector. The commonality is a kind of ancient wish to do good.

What are your long-term defense strategies for the NGO sector?

The long-term defense is around cyber deterrence. One, we should increase the technical cost of cyberattacks, meaning enhancing the cybersecurity maturity of organizations so that it's no longer tempting to attack them. That's the CyberPeace Builders program and we want to bring NGOs to that level of defense. That's difficult in an era of budget cuts. For NGOs, cybersecurity never was a top priority. Now, particularly amid steep cuts in Europe and in the US, it is even further down the list.

> “WE NEED TO PUT SOME FEAR IN THE ATTACKER AND THERE IS NO FEAR WITHOUT ACCOUNTABILITY. WE NEED STATES TO MAKE ATTACKERS UNDERSTAND THAT THEY FACE A RISK IN PUSHING THAT BUTTON.”

Second, we need to put some fear in the attacker and there is no fear without accountability. We need states to make attackers understand that they face a risk in pushing that button. This is why we provide data to support national and transnational accountability work. If states live up to the challenge, attackers should see soon that there is a credible threat for their crimes.

Broadly speaking, can cybersecurity stay ahead of cyber assaults?

That's kind of a tough one. But I'm optimistic because I decided to be and because it is what I need to stay in action. Let's look at the glass half full. In a few years, we supported hundreds of NGOs, created a unique cooperation with the private sector and we sourced volunteer expertise from cybersecurity, data science, AI engineering, policy analysis, all working together to create and accomplish something meaningful.

Across the globe, private sector experts are saying, “Of course I want to help,” at a time when the general impression is that everyone is burned out and cannot do anything anymore.

I am also optimistic because the world is going through such a crisis. Sometimes a wake-up call can produce a better result than a slow and insidious threat.

Optimism—it may be only a posture, but let's remain optimistic.

Is there anything else you want to share that we haven't discussed?

There is a broader point about systemic change. We help individual NGOs protect themselves and we partner with cybersecurity companies. But we remain independent in our technical stack and do not depend on any specific company to implement our capabilities. We built, in-house, our end-to-end analytical process. That's important because we want to remain independent.

As part of our broader mission, we are using the data and knowledge we gain to advocate for what we call Cyber Peace—policies that will result in a cyberspace that ensures that the fundamental rights and freedoms of people and organizations are respected and is governed by the rule of law that is human-centric.

Learn more or volunteer with CyperPeace Institute at www.cyberpeaceinstitute.org. ◆

MARK SEIFERT is a Partner in Brunswick's Washington, DC office and co-Chair of the firm's global Cybersecurity, Data & Privacy practice.