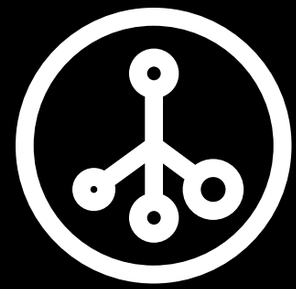

DIGITAL
PEACE
NOW
2020
CITIZENS ON
CYBERATTACKS
The Digital Peace Now Society's
International Cyberwarfare
Awareness Report

The statistics and data in 'Citizens on Cyberattacks' give a true look at, and meaningful snapshot of, the digital age in 2020. This report is for the global public, business leaders, governments, advocates, and changemakers alike.

– RAJ BURLI, DIGITAL PEACE NOW SPOKESPERSON



INTRODUCTION

The Digital Peace Now Society's International Cyberwarfare Awareness Report is an annual international snapshot of the public's awareness of and attitude towards the dangers of nation-sponsored cyberattacks.

In recent years, nation-sponsored cyberattack targets have included governments, critical infrastructure, medical facilities, and private businesses throughout the world. Governments have struggled to reach an international "rules of the road" agreement that clearly define parameters for nation-backed online hostilities. As these attacks continue to grow in sophistication and scale, gauging the public's understanding of the threat can help leaders understand their citizens' sense of urgency around the issue, as well as, help identify ways to engage the public in the conversation.

Key insights include digital citizens' perceptions of cyberattacks, expectations of their governments to address cyberattacks, possible approaches to curb cyberwarfare, as well as a glimpse at the growing impact of interconnectivity in their personal lives.

METHODOLOGY

Between May 15–27, 2020, PSB conducted an online survey in six different countries, focused on gauging current awareness of the dangers of cyberattacks by foreign countries and identifying support for "Digital Peace" related initiatives to curtail it.

This was a follow-up study to work commissioned in 2018, tracking relevant perceptions and attitudes over time to highlight the importance of cyber threats and reveal broad support for action at the international level.

COUNTRIES POLLED

France
Mexico
India
Malaysia
South Africa
United States

1,500

online consumers per country (±2.43)

AGES

18-64

with demographic representation

BIGGEST TRENDS

WE ARE CONCERNED

- One-third of people polled have had a personal account hacked.
- Most are comfortable comparing the threat of nation-sponsored cyberattacks to the threat of nuclear attack.
- 9 in 10 agree our way of life is at risk if nothing is done to address the threat of cyberwarfare.

THE THREAT FEELS VERY REAL

- Those polled from larger nations tend to assume their country is conducting cyberattacks against other nations.
- Cyberattacks against elections are among the most commonly recognized types of digital threats.
- Due to COVID-19, there is more awareness of how frequently nation-sponsored cyberattacks are unleashed.

GLOBAL SOLUTIONS WANTED

- Most back the idea of governments working together with the tech industry to stymie nation-sponsored cyberattacks.
- There is wide support for a global cyberwarfare "rules of the road" agreement — with some differing ideas on the specifics.

THE DIGITAL AGE IS HERE ... AND SO ARE THE THREATS

THE TAKEAWAY

We rely on the internet more than ever, but have yet to address the vulnerabilities of global connectivity.

FROM THE DATA

~1 IN 3 PEOPLE HAVE HAD A PERSONAL ACCOUNT HACKED.

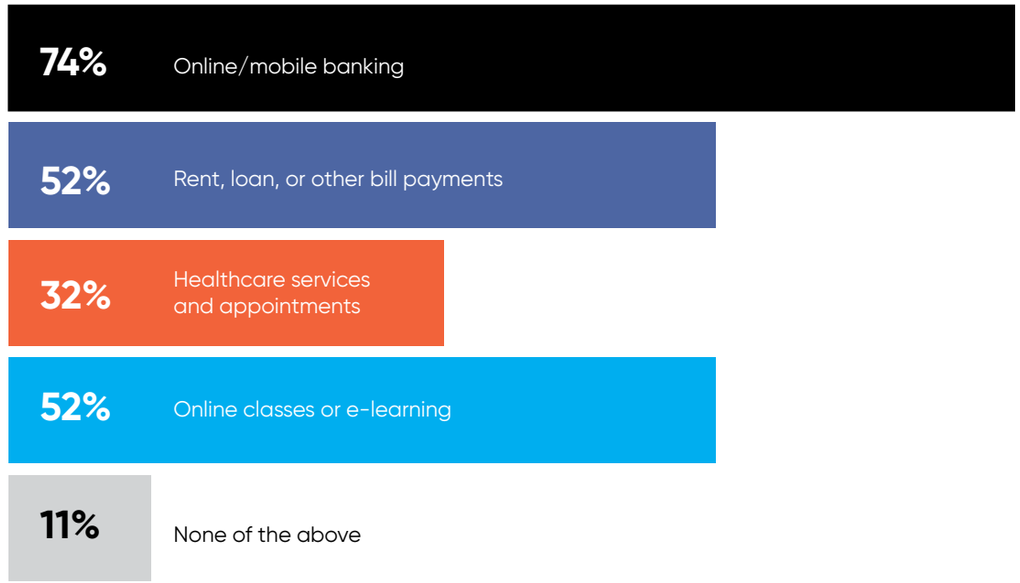
THE DIGITAL AGE IS HERE ... AND SO ARE THE THREATS

Right now, more than half of the world's population is online. With so many relying on the internet, it's imperative that we keep it safe, reliable, and accessible.

However, the internet is still incredibly vulnerable. A major cyberattack that impacted our ability to maintain our online activity would have huge repercussions on society.

This translates to an urgent need to address the threat of cyberattacks and secure the safety of the internet.

We often conduct necessary activities online.



96%

Say internet access is important in their daily lives.

2-8 hrs

Average time spent online every day.

1 in 3

Have had a personal account hacked.

THE MORE WE KNOW, THE MORE WE'RE CONCERNED

THE TAKEAWAY

The threat of cyberattacks is already alarming—and the more we understand, the more intensely concerned we become.

FROM THE DATA

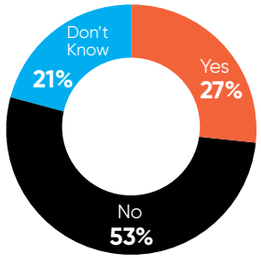
~84% OF PEOPLE CONSIDER THE THREAT OF CYBERATTACKS TO BE ON PAR WITH THE THREAT OF NUCLEAR WEAPONS.

THE MORE WE KNOW, THE MORE WE'RE CONCERNED

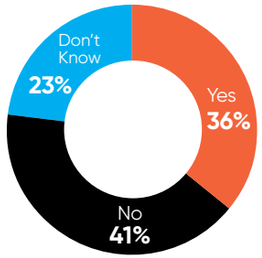
Generally, we're not just aware of cyberattacks, we're already concerned about their impact and suspect our governments are using them against other nations.

When given details of specific attacks, including those targeting governments, financial institutions, and, recently, healthcare centers during COVID-19, our concern that the safety and stability of the modern world are at risk intensifies.

As more of us gain a better understanding of cyberwarfare, there will be a stronger call for world leaders to take action to stop it.



Aware of specific attacks on your own country



Aware of specific attacks on other countries

52%

Acknowledge that their own governments launch cyberattacks on other countries semi-regularly.

84%

Are comfortable comparing the threat of cyberattacks to the threat of nuclear attack.

Top emotions when informed that critical infrastructure has been targeted by cyberattacks

1. **Shocked** (46%)
2. **Horrified** (44%)
3. **Outraged** (34%)
4. **Anxious** (32%)
5. **Annoyed** (30%)

Top 5 Highly Concerning Attack Targets

1. **Financial Systems** (23%)
2. **Government Organizations** (17%)
3. **Nuclear Power Facilities** (12%*)
4. **Election and Voting Systems** (6.5%)
5. **Connectivity Infrastructure** (6.5%)

**No data For Malaysia*

TEAMWORK MAKES THE DREAM WORK

THE TAKEAWAY

Continuing to tolerate cyberwarfare is not an option—and the path to a global solution will be a multistakeholder approach.

FROM THE DATA

~3 IN 4 PEOPLE SUPPORT JOINING AN INTERNATIONAL AGREEMENT WITH "RULES OF THE ROAD" AROUND GLOBAL CYBERWARFARE.

TEAMWORK MAKES THE DREAM WORK

As we face the growing threat of cyberwarfare, we can't help but question if our governments are prepared to address the threat alone.

Given this, it's no surprise that there is broad public support for collaborative solutions that bring together governments, civil societies, and private industry, towards global rulemaking around cyberwarfare.

71%

Believe their government is responsible for protecting their country from cyberattacks.

VS.

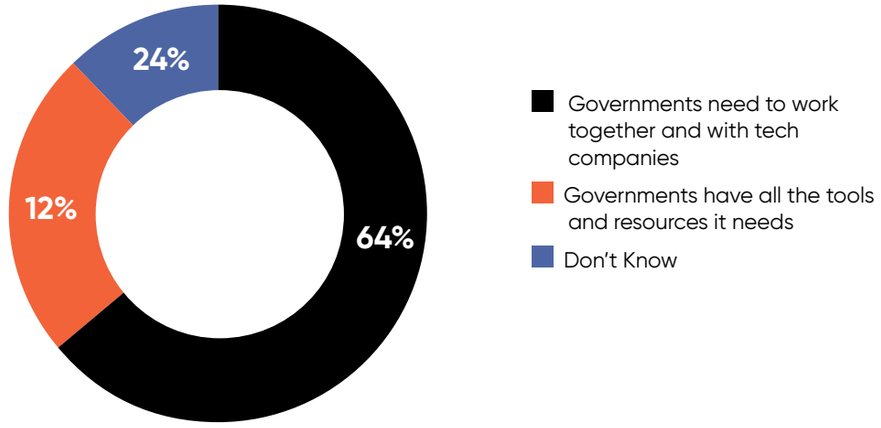
50%

Believe their government is able to protect their country from cyberattacks.

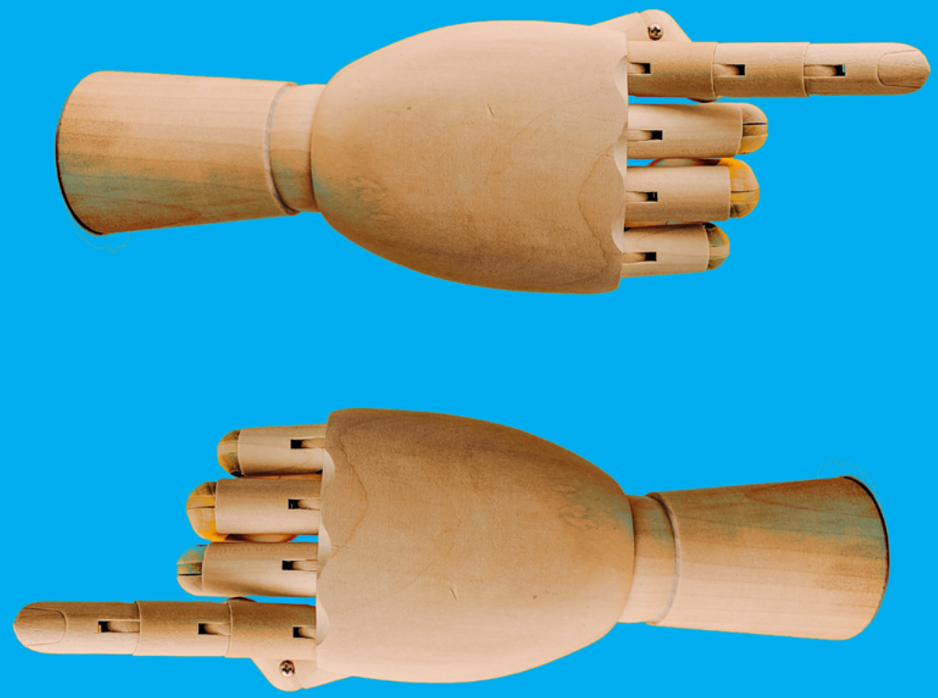
85%

Believe a global "rules of the road" agreement around cybertechnology is needed.

Most back the idea of governments working together with the tech industry to stymie cyberattacks.



REGIONAL DIFFERENCES THREATEN COMMON GROUND



THE TAKEAWAY

We perceive multistakeholder agreements as a good solution to curb the threat of cyberwarfare, but differ in our expectations of the exact shape of these agreements.

FROM THE DATA

IN INDIA, 80% BELIEVE THE GOVERNMENT CAN PROTECT THEM FROM CYBERATTACKS—IN MEXICO, ONLY 26% BELIEVE THE SAME.

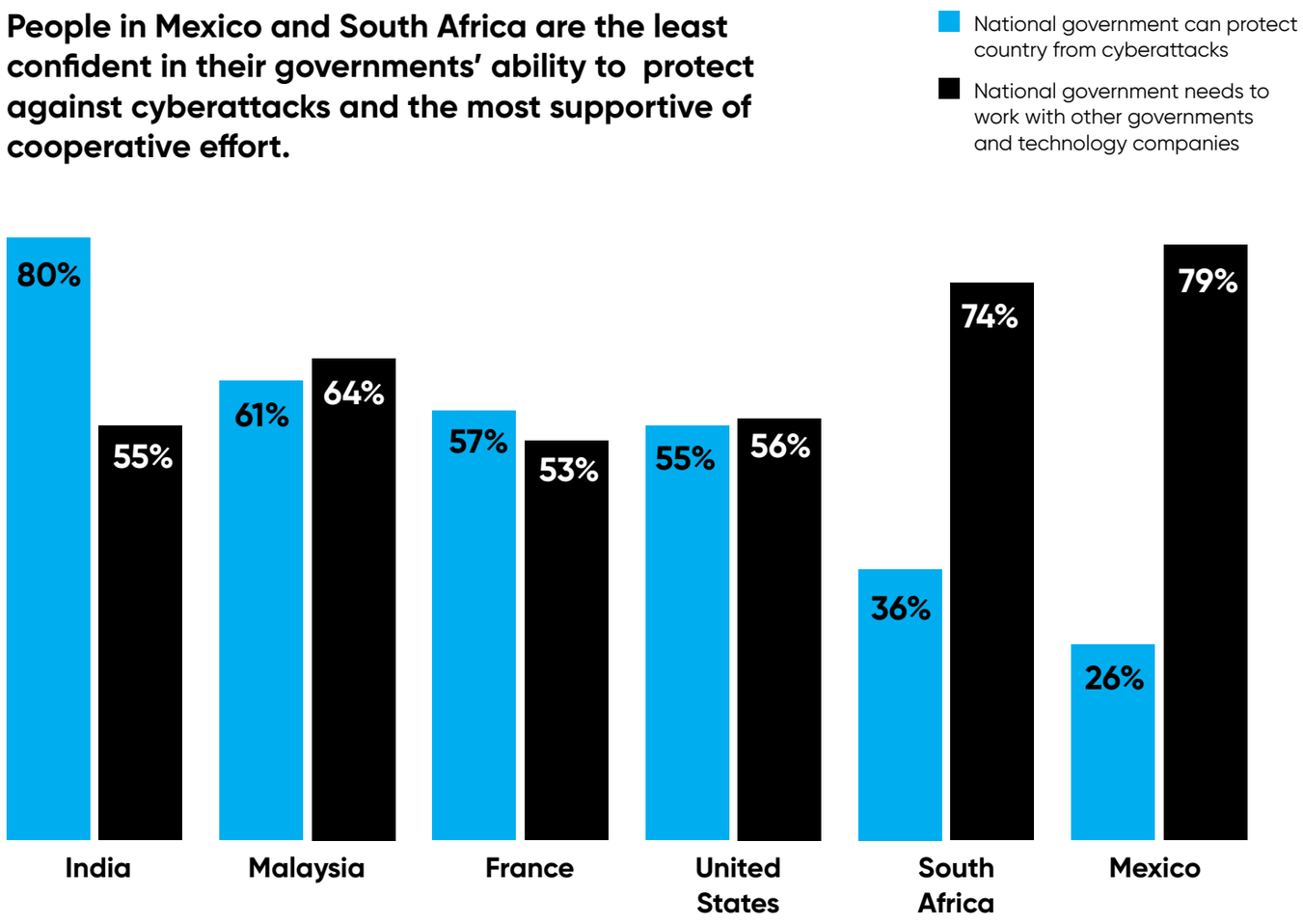
REGIONAL DIFFERENCES THREATEN COMMON GROUND

A collaborative multistakeholder approach towards cyberwarfare presents an opportunity to prevent a future where countries are devastated by cyberattacks. This is especially important for nations with fewer resources or capabilities to protect themselves.

However, we have different levels of commitment towards an international agreement, despite supporting it, primarily based on regional location and our confidence in government.

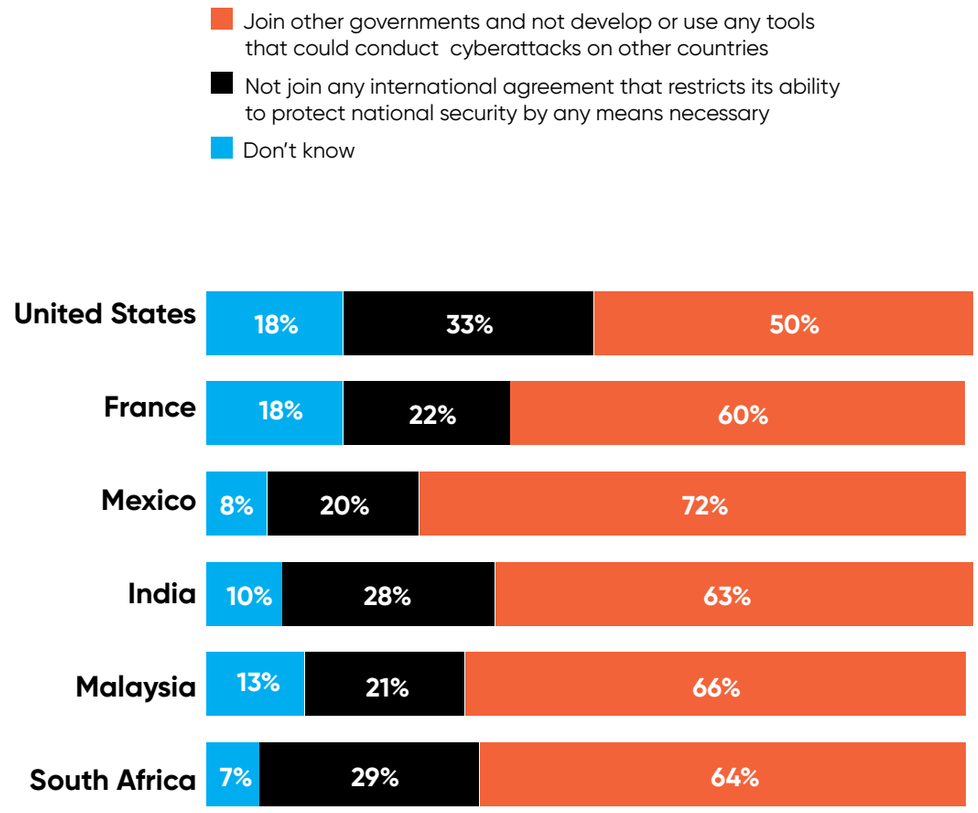
This disparity shows multistakeholder solutions should be rooted in enhancing, not detracting from, the role of national government.

People in Mexico and South Africa are the least confident in their governments' ability to protect against cyberattacks and the most supportive of cooperative effort.

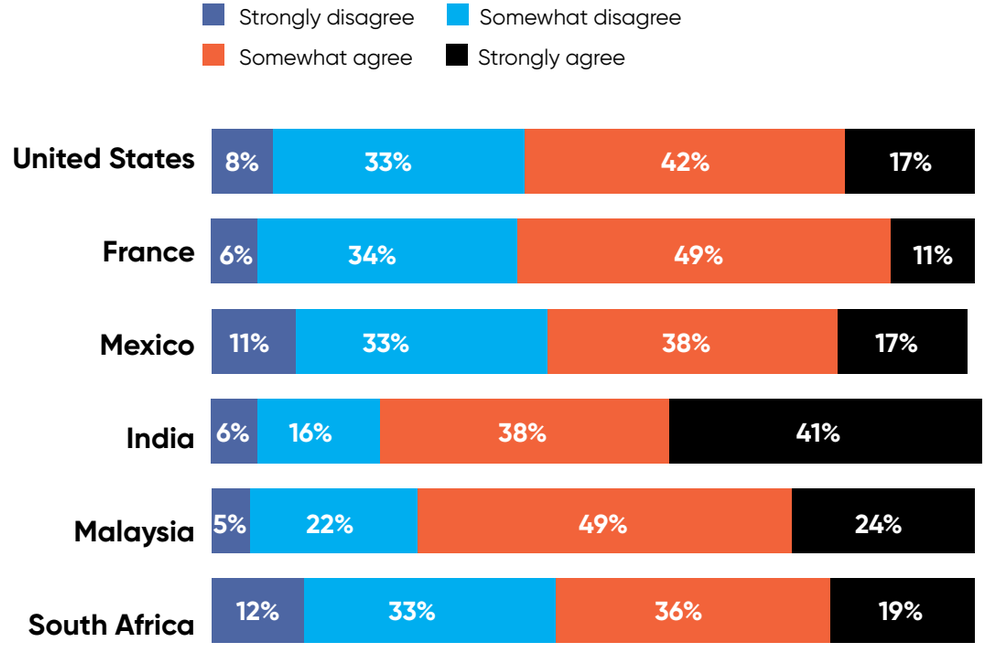


REGIONAL DIFFERENCES THREATEN COMMON GROUND

My government should...



Agreement that individual countries are better equipped to combat cyberattacks by a foreign country than any international watchdog or global agreement varies by nation.



DEFEND DEMOCRACY FROM DIGITAL DISRUPTION

THE TAKEAWAY

Ensuring the safety and security of democratic elections is critical as our world continues to experience rapid technological advancement.

FROM THE DATA

28% IN THE U.S. KNOW ABOUT CYBERATTACKS ON ELECTIONS, MAKING IT THE COUNTRY'S MOST RECOGNIZABLE NATION-SPONSORED CYBERATTACK.

DEFEND DEMOCRACY FROM DIGITAL DISRUPTION

The intersection of technology and elections has been an attractive target for many state-sponsored cyberattacks. Allegations of Russian interference in the 2016 U.S. presidential election brought the threat into the public spotlight. This has resulted in persistent and urgent concern that digital technology can be used to undermine democracy.

To protect our elections and democracies, we need to address this threat immediately because a major attack could have deep and long-lasting repercussions.

I read somewhere that Russia interfered during the elections in the United States
– Citizen of South Africa

Top 3 countries perceived as most responsible for cyberattacks (including election interference-related attacks)

1. **China** (39%)
2. **United States** (29%)
3. **Russia** (22.5%)

Cyberattacks against elections are among the most commonly recognized types of digital threats.

5x

Amount by which the knowledge of electoral cyberthreats is greater than threats of COVID-19 vaccine hacking in the United States.

Russia's attack on the United States during the last presidential election
– Citizen of Mexico

HEALTHCARE IS CAUGHT IN DIGITAL CROSSHAIRS

THE TAKEAWAY

The wave of cyberattacks during COVID-19 has brought an uptick in public awareness of cyberwarfare.

FROM THE DATA

25%–50% OF OUR ROUTINE HEALTHCARE TASKS, INCLUDING PRIVATE TELEMEDICINE VISITS, OCCUR ONLINE.

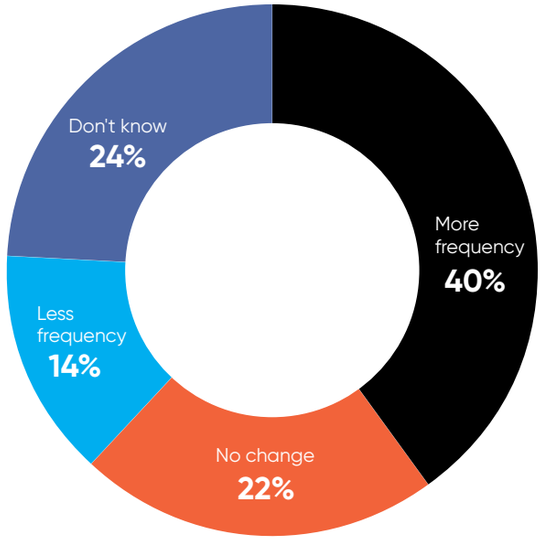
HEALTHCARE IS CAUGHT IN DIGITAL CROSSHAIRS

Amid a global pandemic, we've witnessed more cyberattacks on hospitals, healthcare networks, testing facilities, and research centers.

Even though cyberattacks on hospitals have always caused anxiety, the sheer volume and scope of these attacks sent shockwaves around the world.

As we move more healthcare services online, we must protect them from the threat of cyberattacks, or we'll risk extreme crises when we are at our most vulnerable.

Most fear cyberattacks are happening more frequently during COVID-19.



46%

Percentage of respondents from India who use the internet for healthcare services and appointments.

When prompted for specific examples of cyberattacks, COVID-19 vaccine hacking is one of the most often named.

"China trying to steal virus vaccine information"
– Citizen of United States

"If I'm not mistaken, the US government has recently been attacked due to the COVID-19 pandemic"
– Citizen of Malaysia

"For the Corona virus vaccine"
– Citizen of France

CONCLUSION

THE THREAT IS URGENT

We are aware of the growing trend of sophisticated cyberattacks that hints at a future where the internet is compromised by cyberwarfare.

ENOUGH IS ENOUGH

The alarming number of attacks on medical facilities, elections, governments, and financial institutions are cause for great concern and anxiety. We are looking at our leaders for solutions to get us off this dangerous path.

GLOBAL PROBLEM: GLOBAL SOLUTION

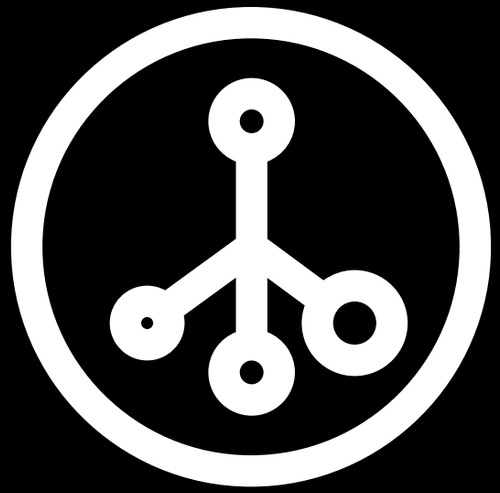
There is strong public support for international multistakeholder agreements that include security benefits and additional support and resources for each partner nation.

DIGITAL PEACE NOW

Digital Peace Now is a global movement dedicated to protecting the internet from becoming a battlefield. Our supporters include citizens from over 170 different countries who celebrate the internet and look to it for connection, opportunity, and inspiration. With a firm belief that there is no peace without digital peace, our goal is to build a society of empowered citizens who understand the threat of cyberwarfare and demand that world leaders ensure the safety of our online world.

psb

PSB Research is a global insights and analytics consultancy rooted in the science of public opinion, serving blue-chip corporate and political clients in over 200 countries. For over 40 years, PSB has provided actionable insights and counsel to help clients address their most complex challenges and win in highly competitive situations. PSB serves Fortune 100 corporations, governments and associations, and has helped elect more than 30 presidents and prime ministers around the world. PSB is a member of the BCW Group of companies, which is a part of WPP (NYSE:WPP), a creative transformation company.



DIGITALPEACENOW.ORG