14

Crowdsourcing Cyber Peace and Cybersecurity

Vineet Kumar

1 INTRODUCTION

The Internet's potential can help people from across the globe collaborate and share information for a common cause. Every year, tens of millions more individuals and businesses join cyberspace. However, this newfound access brings in its own set of vulnerabilities, threats, and risks. Crowdsourcing is one way to address these risks by using a systematic approach that makes use of the capabilities of the Internet and its users. When vital information and valuable expertise are shared between people and organizations using crowdsourcing for cybersecurity purposes, it can bring forth positive results for the benefit of all. The CyberPeace Corps is one such crowdsourcing initiative tapping into the skills, expertise, and passions of individuals and groups from all backgrounds to establish cyber peace by collectively building resilience against cybercrime and cyber threats, while upholding the cybersecurity triad of confidentiality, integrity, and availability of digital information resources. Through the crowdsourcing model of the CyberPeace Corps, the idea of a truly global Internet that is trustworthy, secure, inclusive, and sustainable is furthered by leveraging the potential and possibilities of information sharing and collaboration of a large number of people from all over the world.

2 WHAT IS CROWDSOURCING?

The term "crowdsourcing" originates from a collocation of two words – "outsourcing" and "crowd." Simply put, crowdsourcing concerns obtaining information, seeking opinions, and getting the work done with the help of many people who submit data using the Internet as a medium, using the various tools available, such as social media and smartphone apps (Hargrave 2019). People involved in crowdsourcing can be paid freelancers or those who work voluntarily. There are a lot of processes that can take place. However, six identified forms are as follows:

https://doi.org/10.1017/9781108954341.014 Published online by Cambridge University Press

1. Crowd innovation
2. Crowd funding
3. Crowd voting
4. Crowd creativity
5. Crowd collective knowledge
6. Micro working (Hargrave, 2019)

A simple example of crowdsourcing would be a traffic app that encourages drivers to report traffic jams or accidents, thereby providing real-time, updated information to other app users. This allows people to save time, take the correct route and, most importantly, be safe during their journey. Some of the crowdsourcing benefits are as follows:

- A wider talent pool is available for getting the work done and can contribute to the cause.
- People can work virtually from anywhere, allowing them the flexibility to choose the location and type of work.
- Various enterprises of different resources and interests can tap into an enormous array of skills, resources, and expertise without incurring significant overheads.
- It also enables businesses to raise a large capital pool for special projects.

The point is that crowdsourcing involves breaking down a complicated project into small achievable tasks that a crowd of people can individually work on to achieve set objectives.

3 CROWDSOURCING CYBERSECURITY

The crowdsourcing cyber conflict model is not a new concept. The 2007 Estonia incident, one of the first and most notable DDoS (Distributed Denial-of-Service) attacks in history, is still fresh in cybersecurity circles (McGuinness, 2017). Malicious actors crowdsourced a series of massive attacks on the Estonian infrastructure, paralyzing the entire city, its largest banking network, and the Parliament (McGuinness, 2017).

But what is interesting is the way Estonia established a model of the first of its kind volunteer cyber force, called the Defence League Cyber Unit (CDL), in 2010. The unit is part of the military in Estonia, but is essentially a civil body with members of the public and private sectors enrolling as experts who render support in the times of a cyber crisis. It started as an initiative during the 2007 attacks, but was capitalized on by Estonia through the institutionalization of the volunteer force into a unit within the military. What this goes on to say is that if crowdsourcing can be used to cause cyberattacks of such a massive magnitude, it can prove useful in fighting cybercrimes as well. Among many others, this incident paved the way for conceiving the creation of a CyberPeace Corps model.

https://doi.org/10.1017/9781108954341.014 Published online by Cambridge University Press

4 WHAT IS THE CYBERPEACE CORPS?

The CyberPeace Corps is a volunteer-driven initiative by the CyberPeace Foundation for building peace in the cyber world. It is a coalition of citizens, experts, and students who volunteer to come together for sustaining cyber peace. The concept continues to evolve, but it involves a "crowd of" diverse people comprising citizens and organizations who converge as working groups or individual volunteers to foster cyber peace in marginalized communities, organizations, and nations around the world. Currently, over 1,200 CyberPeace Corps members are spread across forty countries are working to enhance their technical capacity against cybercrimes and threats using various modes of communication like social media, street theaters, workshops, webinars, and so on among communities at national and global levels. They also provide support in data collection and analysis to back the training modules developed for workshops, detecting cyberattacks, using machine learning for investigative analysis, and even assist in content creation and dissemination among other activities. The CyberPeace Corps works mainly across four verticals including: Inclusion & Outreach, Collaboration & Connect, Policy & Advocacy, and Innovation & Outreach related to all aspects of cyber peace and cybersecurity. The CyberPeace Corps focuses on the collaboration of people, even from nontechnical backgrounds to build a resilient, safe, and sustainable cyberspace. The CyberPeace Foundation conducts training program for all volunteers who join the CyberPeace Corps and makes them sign a ten-part oath to promote values to ensure peace in cyberspace and strive hard to achieve them. Imagine what malicious actors will do if they manage to access confidential and sensitive information about a country's defense organization. The consequences of such a scenario could be devastating, not only for the organization but also for the common people. On the contrary, suppose a law-abiding citizen gets information about a planned terrorist attack in the country – s/he would report the same to the law enforcement agencies.

Here lies the benefit of crowdsourcing. Crowdsourcing helps create a faceless army of volunteers who can play a stellar role in protecting society from harm. Looking at the scenario from a cybersecurity angle, it is a massive army that helps fight cyber threats on a large scale. The CyberPeace Corps works on this concept of encouraging people to volunteer and fight cybercrime for the good of all. The CyberPeace Foundation has also been working in building a model for children, as well by establishing CyberPeace Clubs in schools. Under the guidance of faculty, school administration, and team at CyberPeace Foundation, students are trained in conducting sessions on cyber safety and also have a continuous dialogue with other students on a resilient and safe cyberspace.

5 HOW CAN CROWDSOURCING WORK IN CYBERSECURITY?

Authorities, police, and agencies have always used crowdsourcing to combat crime in the physical world. The Boston Marathon bombing investigation (Ackerman, 2013)

https://doi.org/10.1017/9781108954341.014 Published online by Cambridge University Press

and the Broward County Sheriff case (Contributor BP, 2011) are two prime examples. The public shared media online in large numbers to help the authorities with their investigations. A similar methodology can be used for the purpose of ensuring cybersecurity. There are three prominent fronts where crowdsourcing can help cybersecurity, as discussed below:

- *Collaboration*: People from various locations and different walks of life can put their heads together for a common cause. They can share ideas, work together as a team to bring forth something creative and useful to thwart cybersecurity issues, and offer productive involvement in a cybersecurity project. Synack is an example of one such group of experts ready to respond to organizations' calls and become involved in handling cybersecurity crises so as to combat threats.
- *Sharing Intelligence*: Many experts in the cyber world can contribute vital information to protect numerous people and organizations from serious cyber threats. ThreatExchange, started by Facebook, is an example of an intelligence-sharing platform.
- *Bounty Programs*: These are experts who are not permanent employees of large organizations such as Microsoft, Google, or Apple, but still help them. They can offer their expertise in troubleshooting various organizations' software products to find serious flaws or bugs that can prove fatal sooner or later once discovered by malicious actors. They research independently to identify zero-day vulnerabilities and share valuable information with the organization, thereby helping it develop a patch program and save millions of dollars in the bargain.

6 CROWDSOURCING RESEARCH

Crowdsourcing encourages people from different walks of life to contribute their ideas, based on their usage and expertise, to ensure that diversity of thought processes are accounted for. The CyberPeace Corps has already been employed in various cyber research projects using this method. Involving the public in research has the following advantages:

- Researchers get a chance to understand the public's perspective by involving them.
- Similarly, the public can improve their scientific understanding by participating in the research programs.
- CyberPeace Corps platforms provide the right opportunities for people who want to discover projects or researchers who wish to create new projects.
- It allows various people from diverse fields to assist in cybersecurity tasks for the Corps without enrolling as permanent workers.

As the CyberPeace Corps is a volunteer-centric organization, it relies on community support and participation. There is tremendous potential in the community yet to

https://doi.org/10.1017/9781108954341.014 Published online by Cambridge University Press

be tapped. Because there is a severe shortage of cybersecurity professionals capable of handling cyberattacks and related threats, it becomes more relevant to involve the community in projects. Therefore, an initiative like the CyberPeace Corps can help people to contribute their skills and intelligence for the benefit of all. These initiatives have delivered successful results, thanks to collaborative problem solving. Ideas can virtually spring from anywhere, including people not connected to the organization in any way.

7 SERVING SOCIETY

The CyberPeace Corps can help business entities by educating the organization's employees to maintain cybersecurity hygiene. The Corps volunteers are always on the move from one organization to another to drive home the fact that it pays to maintain cybersecurity hygiene. It could be educating people on maintaining strong passwords and discouraging them from sharing them with others to helping people deal with the aftermath of a cyberattack.

The CyberPeace Corps believes in people maintaining self-discipline when using the Internet for personal or business purposes. A simple sharing of an email id and password is enough to clean out a bank account in no time.

8 CREATING AN IMPACT

The crowdsourcing journey comprises four phases through which a potential volunteer has to pass:

Awareness Phase: The awareness phase is the first phase where an individual discovers the initiative through some channels, such as the Internet, professional networks, or a Corps volunteer.

Consideration Phase: The second phase is the consideration phase, where the volunteer learns more about the initiative and decides whether to be involved in it.

Participation Phase: In this phase, volunteers participate in the research and contribute willingly.

Closing Phase: The final phase is the closing phase, where the initiative's compensation occurs.

The CyberPeace Corps assesses the volunteer's journey through this proven model.

9 CALL FOR ACTION

Today, even government authorities and security agencies have put crowdsourcing into practice. By encouraging crowdsourcing in cybersecurity, talented individuals can showcase their capabilities and help organizations thwart cyberattacks.

- With the industry facing a dearth of cybersecurity professionals, the CyberPeace Corps provides an ideal opportunity for people with the expertise and interest to volunteer to fight cybercrime.
- Interested individuals are welcome to volunteer toward offering their services to the CyberPeace Corps.
- The exciting aspect is that it is not mandatory to have a technical background to volunteer.
- Even people having nontechnical experience can play a critical role in creating cybersecurity awareness among the public.
- Every individual is capable of contributing to safeguarding cyber peace in some way.

As they say, "Security is everyone's responsibility," so here is your chance to connect with the CyberPeace Corps help others to be safe online, and contribute to the greater cause of peace in cyberspace.

REFERENCES

Ackerman, S. Data for the Boston Marathon Investigation Will Be Crowdsourced, April 16, 2013, *Wired*, www.wired.com/2013/04/boston-crowdsourced/

Contributor BP, How a Sheriff Uses His 10,000 Facebook Fans to Solve Crimes, October 31, 2011, Consumerist, https://consumerist.com/2011/10/31/how-sheriff-al-lamberti-uses-his-7200-facebook-fans-to-solve-crimes/

Hargrave, M. Crowdsourcing, July 8, 2019, Investopedia, www.investopedia.com/terms/c/crowdsourcing.asp

McGuinness, D. How a Cyber Attack Transformed Estonia, April 27, 2017, *BBC News*, www.bbc.com/news/39655415

Shackelford, S. The World Needs a Cyber Peace Corps, 2017, *Slate*, https://slate.com/technology/2017/10/the-world-needs-a-cyber-peace-corps.html

Weingarten, D. Born in India, CyberPeace Corps Trains Tacklers of Disinformation, Online Challenges, May 7, 2020, Meritalk, www.meritalk.com/articles/born-in-india-cyber-peace-corps-trains-tacklers-of-disinformation-online-challenges/