My name is Kemal Veli AÇAR. I have been working as a unit manager at the Department of Cybercrime Vof the Turkish National Police since 2014. Before that position, I worked at several different police stations as a mid-level manager. This diverse and extensive experience gave me deep insight into the issues of online and offline child protection. As a result, I drafted five research outputs about online child sexual abuse. At this submission, I will try to cover the prevention and detection aspect of the global fight against online child sexual abuse. For more information about me and my work, please check: <https://www.researchgate.net/profile/Kemal_Acar>

Children should freely express themselves and exercise other essential rights in online environments without being exposed to online threats such as groomers or child abuse materials (CAMs). Therefore, eliminating or minimizing such online threats is an inevitable part of ensuring the well-being of children in cyberspace. Particularly in terms of prevention and detection of online child sexual abuse incidents, the main objective of this submission is to outline the global efforts for creating a safer Internet for the children and evaluate the effectiveness of current measures briefly.

Being well aware of the fact that struggle against online child sexual abuse must be more concerted on a global scale, many different organizations have come together to produce timely and appropriate global responses. From the first World Congress against Commercial Sexual Exploitation of Children in 1996 to the recent WeProtect initiative, people have seen multiple attempts with different titles to steer the global fight against online child sexual abuse toward a direction which is less disorganized and thus more manageable and powerful. In terms of policymaking, legal amendments, raising awareness and public-private collaborations, these efforts have yielded invaluable and unprecedented outputs, particularly compared to other areas of crime fighting. However, the threat landscape and the challenges faced by law enforcement agencies (LEAs) have also evolved to the extent that more efficient measures must be put into practice at a global level.

First of all, at the moment, against the tide of a huge amount of data both in online environments and in seized devices of suspects, LEAs barely manage to focus on undiscovered CAMs to identify victims, abusers, and crime scenes. Considering the viral nature of the Internet, the discovery of a child abuse material and its inclusion into the repositories CAMs take a lot of time and the whole process lacks the efficiency to response the rapid spread of visual materials. US-based prominent Internet service providers such as Facebook, Google and Twitter have robust hash-matching technologies to detect the CAMs in their platforms. And these tech giants inform the National Centre for Missing and Exploited Children (NCMEC) which also serves as the national repository of known CAMs for the US. In case NCMEC discovers a new CAM by other means, the hash-list of known CAMs is updated and Internet service providers obtain it. Despite not being as fast as it could, this good practice must be embraced at a global level. Furthermore, when a digital forensic examiner finds CAMs in seized devices, he/she must send it to another investigator so the CAMs are uploaded to a global repository such as the International Child Sexual Exploitation Database (ICSE DB) or a national one such as the Child Abuse Image Database (CAID) of the UK. The heavy burden of uploading materials to the repositories and identifying the victims lies on a limited number of LEAs. Needless to say, this is a cumbersome process which brings another layer to the already heavy workload of LEA. In the age of big data, the flow of information between LEAs and the repositories must be heavily relied on the principle of automation and cloud computing, not on the traditional and manual methods. The fact that an investigator manually has to pick and upload CAMs to a repository stands in ironically stark contrast with the contemporary challenges faced by LEAs. Moreover, speaking of repositories of CAMs, there are many of them and unfortunately, no one shares their hash-lists of CAMs with anyone. On top of that, instead of promoting to set up a global repository, the current trend is to establish national repositories in every country. As a result, this nation-centric trend unintentionally has turned the global fight against online child sexual abuse into a “champions league’’ which only a few elite countries could afford to enter. In terms of capacity building, there must be other ways for emerging countries to be involved in this global action without pouring their scarce resources. In conclusion, there might be a way to combine the best practices in this area to form a stable and constant global initiative through a single global repository, instead of irregular international gatherings with relatively insignificant outputs and broad statements. Such a forum might also become a venue for developing actionable global policies for other types of online child sexual abuse such as online grooming, sexual extortion and live streaming of child abuse on demand, in a timely manner. Also, the implementation of cutting-edge technologies such as facial recognition and artificial intelligence requires a great deal of technical expertise, financial resources, and unorthodox legal amendments. In terms of endorsement by official authorities and independent fundings particularly, accumulation of forces under the roof of a global repository might create an unprecedented advantage of sailing on insufficiently utilized or previously uncharted areas. For the time being, none of the layers of the global fight against online child sexual abuse have the pecuniary means, political power or scientific knowledge to pursue this kind of futuristic adventures on their own.

Secondly, online threats to children almost show the same patterns regardless of cultural and geographical differences. For instance, in the cases of sexual extortion, the online groomer befriends the victims and obtain the self-produced visual materials of the victim. Then the abuser threatens him/her with distributing the obscene pictures online if the victim doesn’t comply with the request of providing more self-produced materials of himself/herself. Along the same line, in the cases of webcam child prostitution, the parties meet each other mostly through social media platforms and online dating apps. And then, they continue the conservation on popular VoIP (Voice-over-IP) tools. These similarities in the commission of crime also reflect themselves in the possible standardization of the counter-measures for such heinous acts. Therefore, theoretically, it is possible to develop basic yet crucial strategies and tools to combat such emerging online threats at a global level. For example, awareness-raising activities for online grooming and sexting are essential for children to protect themselves from online dangers. And, many local and regional initiatives have been conducted such programmes to inform the children, parents and teachers. Despite all the good intentions, these efforts sometimes lack the scientific basis, they reach to a limited audience in most cases, they are generally not resilient enough to keep up the pace with the ever-changing threat landscape in a timely manner or the content and the execution of the programmes wildly differ even within the same country. In my opinion, with related stakeholders such as pedagogues, a global authority must develop a basic package for the awareness-raising activities and modify it whenever the need arises. Thus, particularly developing countries would embrace it with little cultural changes and they wouldn’t put too much work into creating a new programme from scratch.

Thirdly, and closely related to the facts and reasons mentioned above, the law enforcement response to online child sexual abuse might also be standardized to some extent. Fortunately, the legal background of the countries on this issue has been largely harmonized, thanks to the global treaties such as the UN Convention on the Rights of the Child (UNCRC), Optional Protocol to the UNCRC, the Budapest Convention, and the Lanzarote Convention. Currently, almost all countries criminalized online child sexual abuse in one way or another. There are some legal problems for the criminalization of emerging online threats but still, the overall situation looks satisfying enough. However, due to the complexities of national legal systems, mere criminalization does not remove obstacles from the path to better international cooperation. Secondary legislations of countries might widely differ from each other and create important problems even if countries punish the offenses with identical penal codes. For example, like all cybercrime investigations, obtaining subscriber information from service providers is critical for detecting the offender correctly and rapidly. Differences between countries legal conditions and procedures for this basic but crucial matter sometimes complicate the process. For instance, while investigators of country A obtain subscriber information directly from service providers, their colleagues from country B need a court order to get it. Consequently, country B cannot respond to the requests in the same way as country A does. Naturally, law enforcement agencies prioritize and expedite the legal procedure in the case of high profile incidents. However, the swiftness of these investigations should be a rule, not an exception. There is an undeniable need for deeper legal harmonization of secondary legislation between countries for a more concerted global action. Along the same line, the procedural powers of the LEAs should be updated and harmonized at a global level as well. As new technologies expand and present new means of communication, offenders adapt their modus operandi accordingly. Initially, traditional websites and public chat rooms were popular among online child abusers. Law enforcement agencies could easily identify suspects by examining the traffic data or credit card information of those websites. For chat rooms, sting operations were very effective at revealing online groomers. However, besides these outdated methods, options for offenders have increased and diversified. A vast area of online environments such as social networking sites, peer to peer networks, online gaming sites and darknet can be used to spread malicious content and reach suitable targets. To keep up with this constantly growing and ever becoming more complex threat landscape, appropriate measures should be taken. Although some extraordinary measures such as managing a Tor network website for deanonymizing the offenders and sending actual CAMs in undercover operations exist, the majority of countries seem to be stuck in outdated approaches, methods and legal backgrounds. Possibly, kickstarting with a similar event to the first World Congress, there needs to be another wave of increasing awareness about these new challenges in order to push the world into making a drastic change.

Lastly, no matter how powerful the legal background is, a country must have capable human resources to enforce the law. Therefore, the training of LEAs is a crucial aspect of preventing any country to become a safe haven for online child sexual abuse. At the moment, there are many ongoing capacity building activities of the regional and global organizations such as the Global Action on Cybercrime Extended (GLACY)+ of the Council of Europe and Interpol training courses. In addition, countries give and receive training programmes through bilateral agreements or treaties. Again, the lack of standardization and focus on short-term goals or easily accessible targets strike me as vulnerabilities here. Most of the time, the trainees or receivers of the capacity building activities were selected by the national authorities without carefully planning the next step about the programmes. Such people definitely benefit the training modules but they also should convey these benefits to other stakeholders within the country by appropriate means. In most cases, they even couldn’t or wouldn’t deliver the results throughout the same unit. This issue largely cripples the potential advantages of capacity building efforts and limits the overall beneficiaries to a few lucky groups. Instead of addressing this distribution problem, givers of the activities generally focus on the number of beneficiaries and activities. Therefore, as long as some conferences and training courses are being held with the attendance of some people, nobody bothers about the long-term outcomes and the true efficiency behind the shiny statistics. However, unfortunately, it’s not easy to fix this issue. Surely, some ethical and practical standards might be developed for the givers and receivers, but in the end, such standards would be destined to be followed on a voluntary basis.