

GLOBAL ALLIANCE AGAINST
CHILD SEXUAL ABUSE ONLINE
2015 Threat Assessment Report



Introduction to the Threat Assessment of the Global Alliance Against Child Sexual Abuse Online

In 2012, the Global Alliance Against Child Sexual Abuse Online was launched and now unites 54 member countries in the fight against online child sexual exploitation through their ministers' commitments to pursue four policy targets:

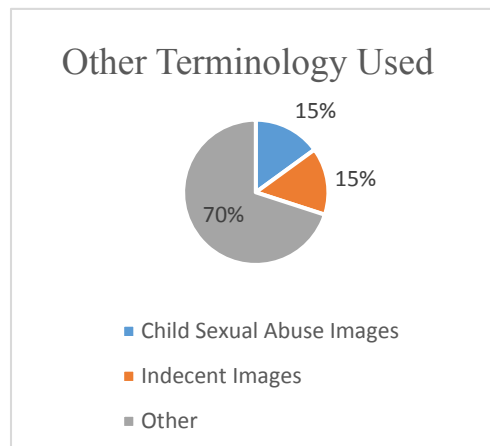
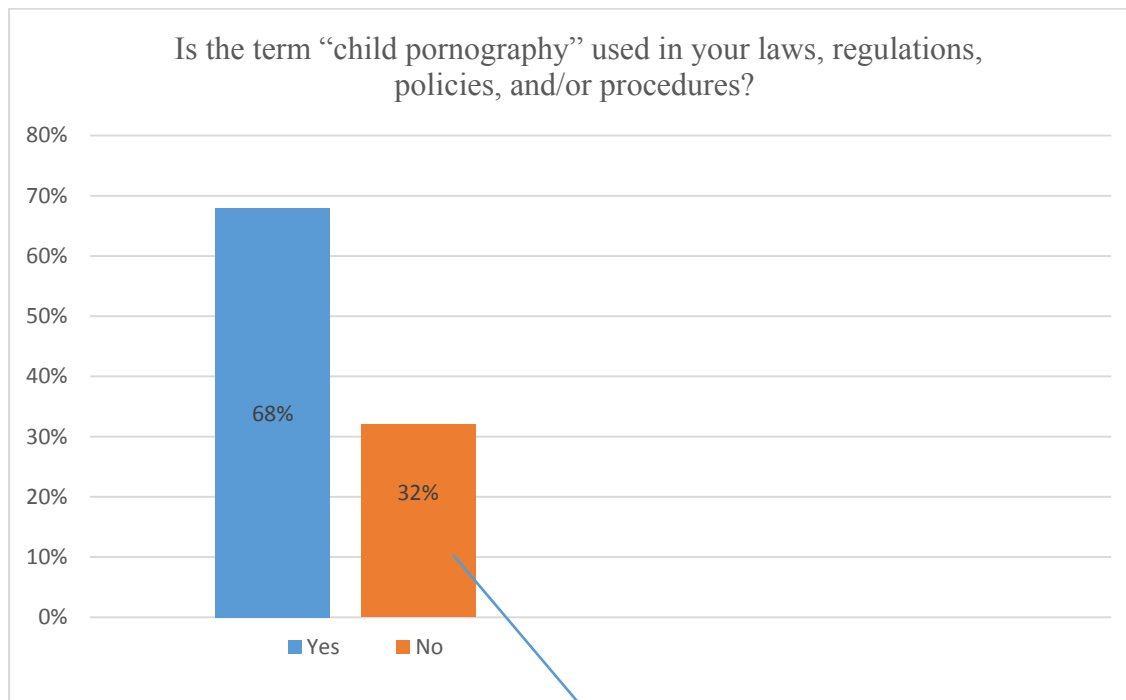
- Enhancing efforts to identify victims whose sexual abuse is depicted in child pornography, and ensuring that they receive the necessary assistance, support and protection;
- Enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders;
- Increasing public awareness of the risks posed by children's activities online, including the self-production of images; and
- Reducing the availability of child pornography online and the re-victimization of children.

In addition to providing biennial reports on their progress in achieving these targets, many Global Alliance member countries also completed a questionnaire to assess the global threat of child pornography and related investigative challenges, and their answers are compiled in this threat assessment report. The objective of this threat assessment is to more fully inform leaders about the nature, magnitude, and global scope of this crime problem, and provide support for the local, national, and international policy changes pertaining to these offenses that are necessary in order to accomplish the shared policy targets.

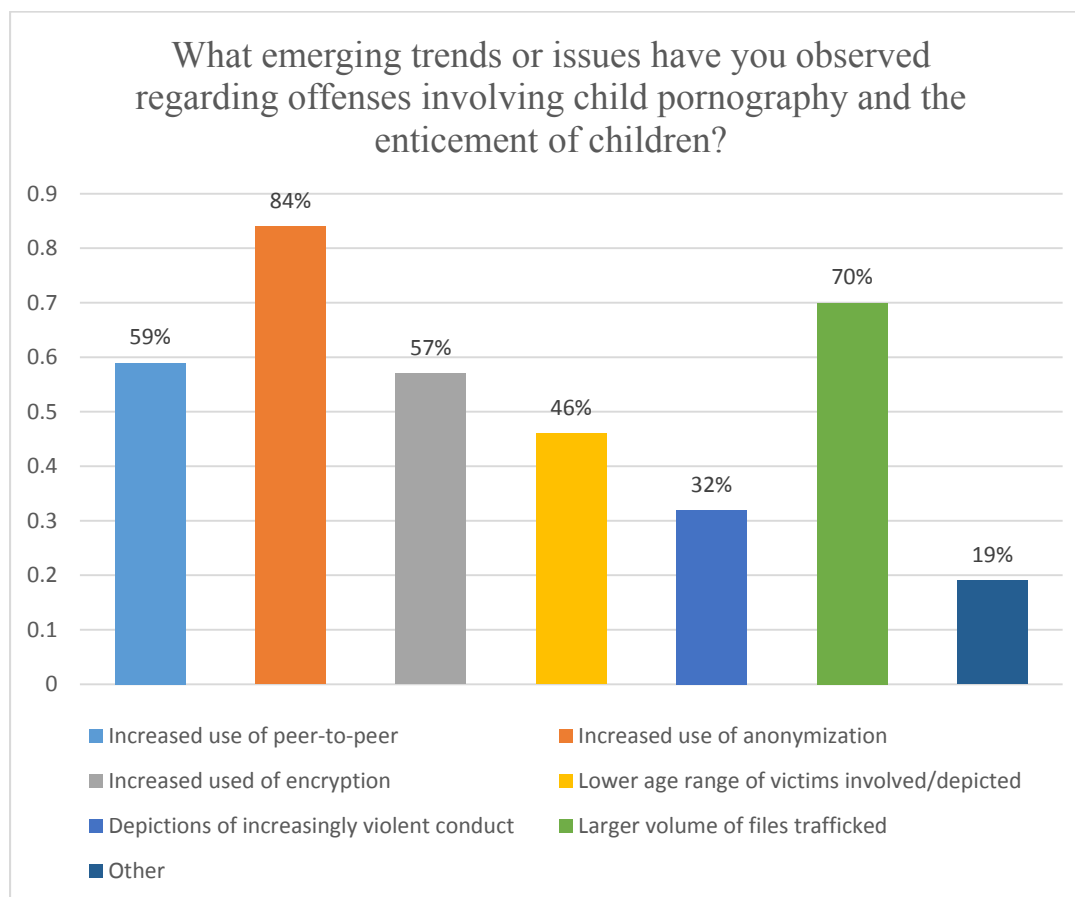
The threat assessment is comprised of four different sections: (1) General Questions; (2) Communications Between Child Pornography Offenders; (3) Technological Issues and Challenges Faced by Law Enforcement; and (4) International Legal Issues and Challenges. Thirty-seven (37) of the fifty-four (54) Global Alliance members responded to the threat assessment questionnaire, which included both quantitative and written responses. Selected written responses are included throughout this threat assessment.

General Questions

Internet child sexual abuse crimes are always changing and evolving, including the legal terminology that is used to describe these offenses. Of the 37 Global Alliance members who submitted responses to the threat assessment questionnaire, 25 indicated that their country used the term “child pornography” in their laws, regulations, policies, and procedures while 12 reported using different terminology, such as “child sexual abuse images” or “indecent images.” Every responding country has laws, regulations, policies, and procedures that address child pornography, whether the term “child pornography” is specifically used or not. The term “child pornography” was defined in the threat assessment questionnaire as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. The term “child” was defined as every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier (definitions are taken from the UN Convention on the Rights of the Child and the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography).



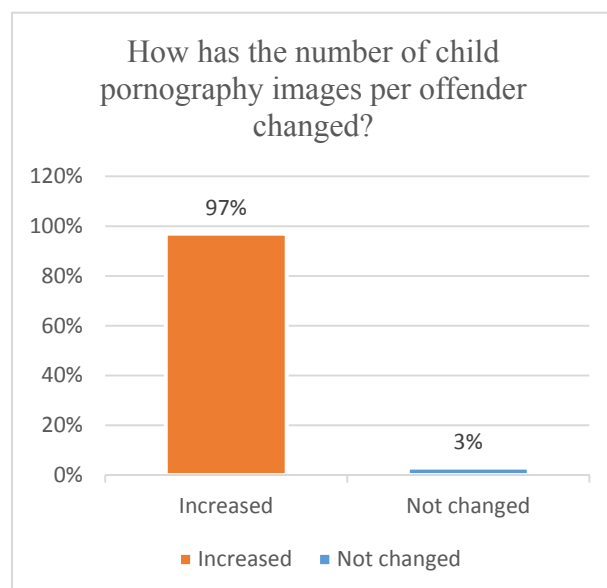
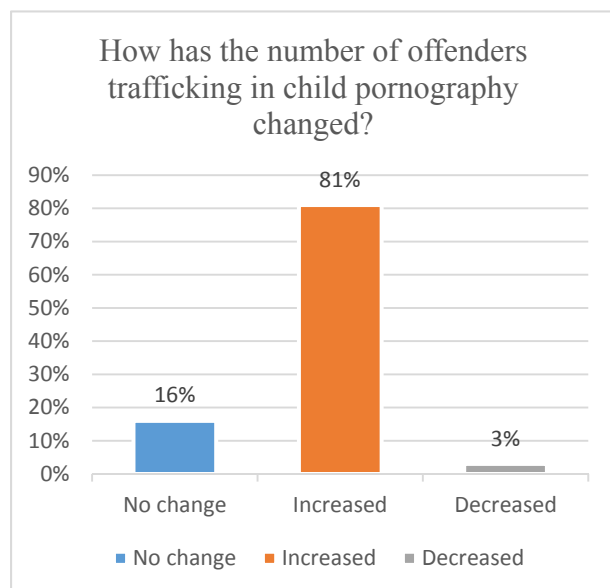
When asked to mark all that apply, the largest emerging trend involving child pornography and the enticement of children, observed by 31 of 37 responding countries, is the increased use of anonymization technology. The term “enticement of children” was defined in the threat assessment questionnaire as the use of digital technology, including the internet and mobile phones, to persuade, induce, entice, and/or coerce an individual who is under the age of eighteen (18) years and located in another country to engage in illegal sexual activity.



Furthermore, 26 responding countries reported an increase in the number of child pornography files being trafficked. Twenty-two responding countries attributed this in part to an increased use of peer-to-peer networks and 21 credited it to increased use of encryption software.

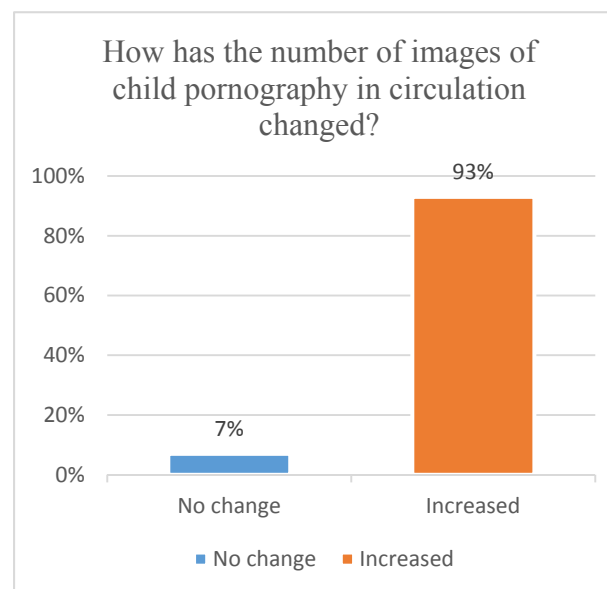
“[With the] increased amount of images being shared amongst teens, children are becoming more daring and explicit, [there is] increased use of registry cleaners and efforts to remove evidence of child pornography from computers, [greater] use of [internet voice and video chat software]/meet ups on photo sharing sites and sharing between two people who meet on such sites. Offenders are involved in guns and drugs, are travelling long distances to meet children who they have enticed online, [and there is a] constant increase in the production of new material, whereas a few years ago, the same set material was being re-circulated”

The volume of child pornography trafficking has increased. The term “child pornography trafficking” refers to the distribution, trade, exchange, sale, receipt, access, or possession of child pornography, including attempts to commit such offenses. Twenty-six of 32 responding countries indicated that the number of offenders has increased, 30 of 31 responding countries asserted that the number of images per offender has increased, and 28 of 30 responding countries indicated that the number of images in circulation has increased.



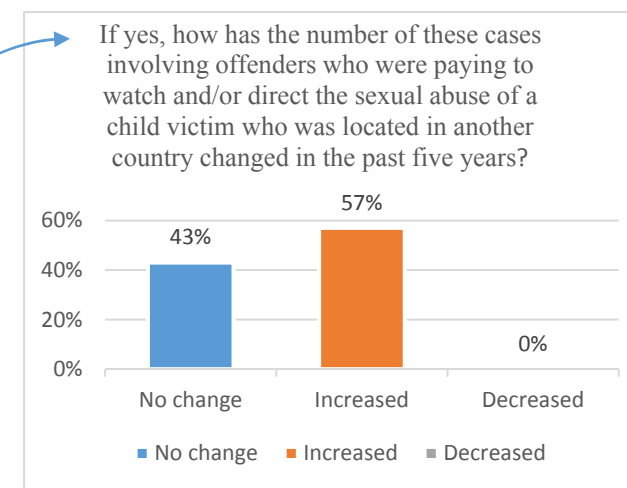
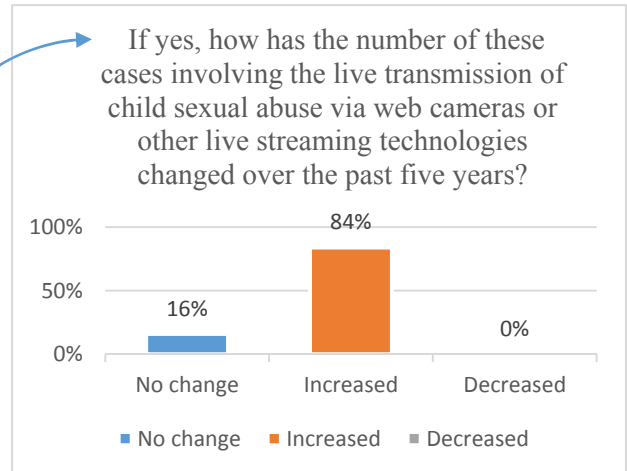
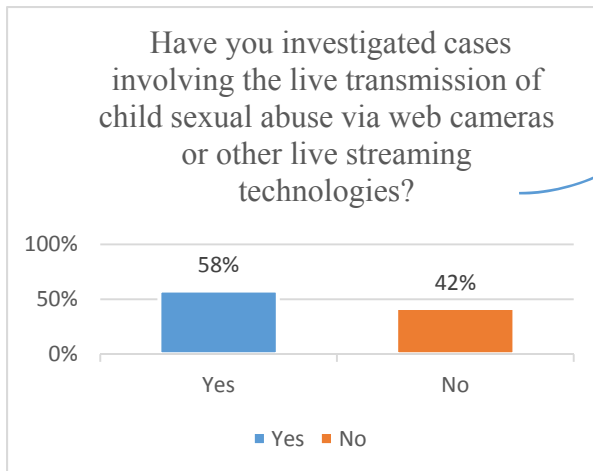
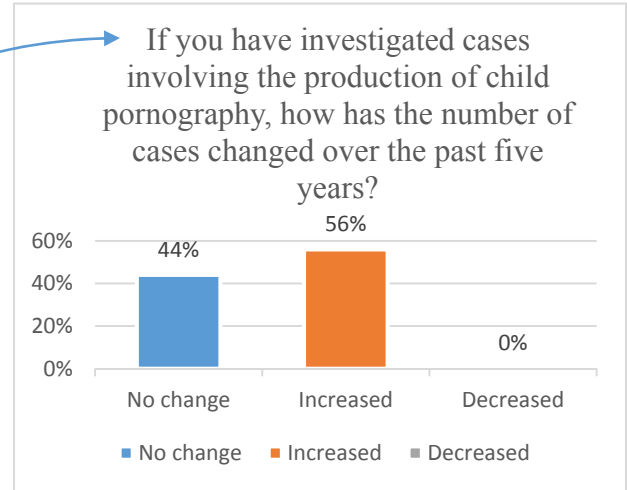
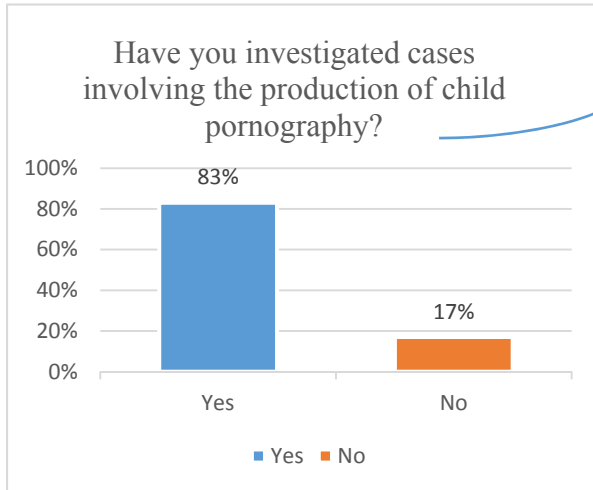
“The volume of child pornography stored has increased because the new storing devices have more capacity”

“Increased use of mobile devices to facilitate offenses has increased the volume of online extortion, featuring demands for self-production of child pornography, and increased live-streaming of real-time sexual abuse of minor victims”



Of the 35 responding countries, 29 had investigated cases involving the production of child pornography. Eighteen of 31 responding countries indicated that the number of child pornography production cases has increased over the past five years. Additionally, 19 of 33 responding countries had investigated cases involving the live transmission of child sexual abuse via web camera and other live streaming technologies. Of the 19 countries that investigated the live transmission of child sexual abuse, 16 indicated that the number of such cases has increased

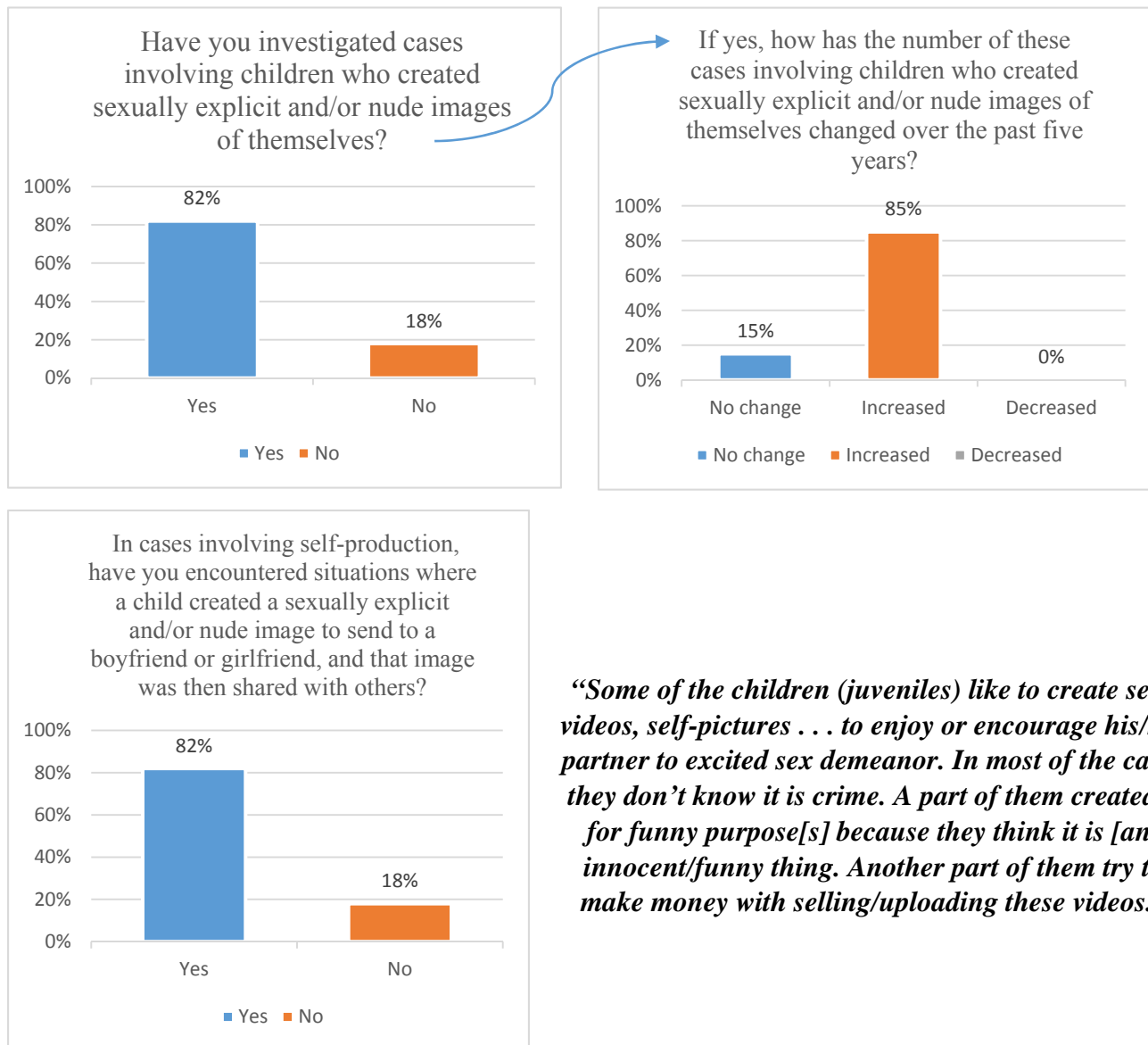
over the past five years. Eighteen of 21 responding countries reported that some cases involved offenders who were paying to watch and/or direct the sexual abuse of a child victim located in another country; 12 countries reported that the trend of such offenders has increased over the past five years.



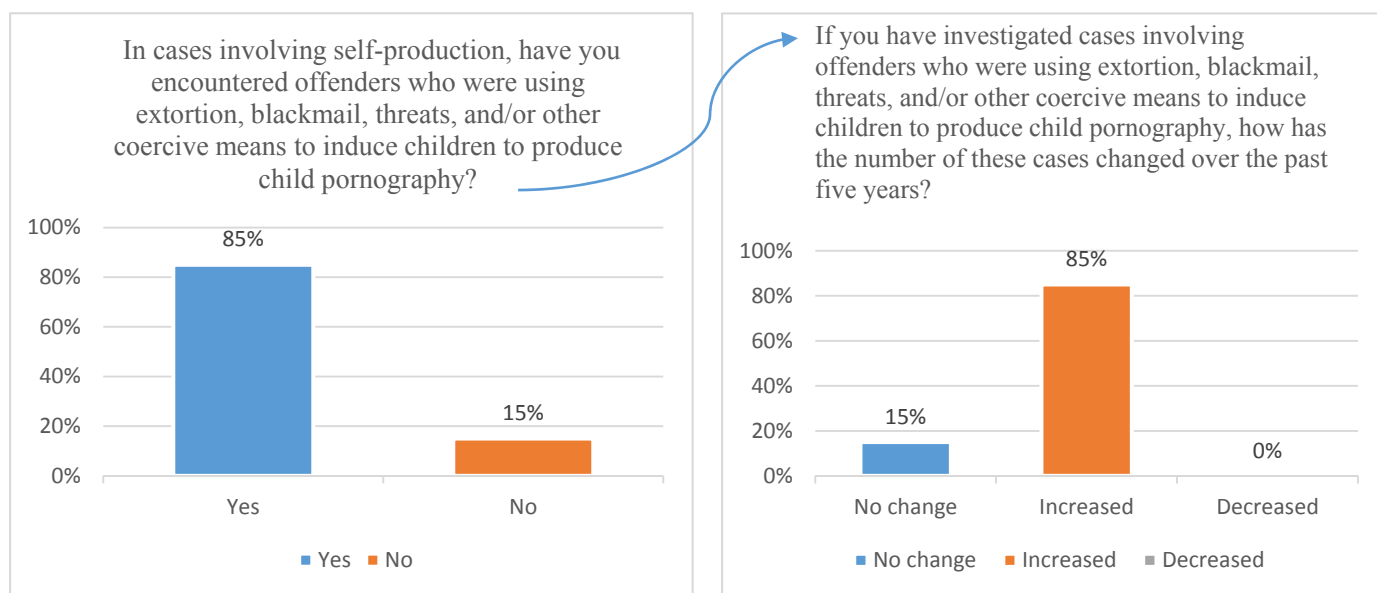
“There has been a significant increase in [offenders who are paying to watch and/or direct the sexual abuse of a child victim located in another country]. Four recent operations identified over 700 suspects worldwide, highlighting the scale of this crime area. Over the next few years, with improved access to high speed internet in countries with high levels of poverty, it is anticipated that this crime type will rapidly escalate.”

* * * *

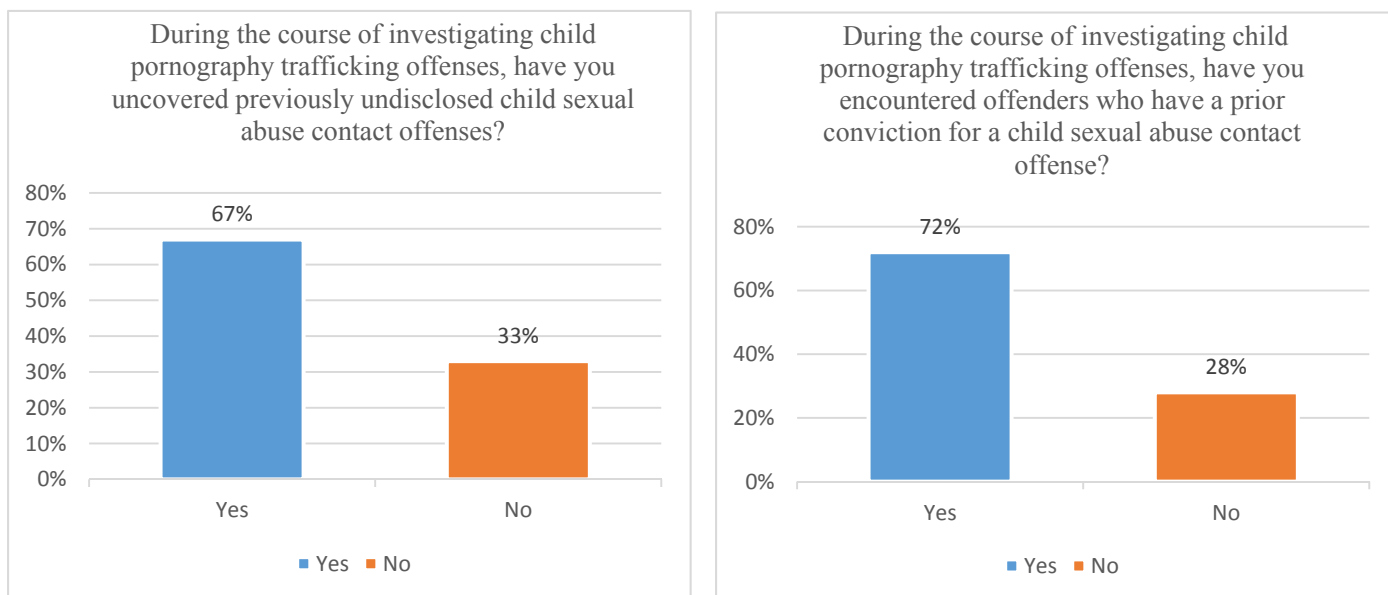
Another trend that has emerged is self-production of child pornography by children. Twenty-seven of 32 responding countries indicated that they have encountered cases involving children who created sexually explicit and/or nude images of themselves. Twenty-three of 27 responding countries saw an increase in the amount of self-production cases in the past five years. Twenty-seven of 33 responding countries reported that they have encountered situations where a child created a sexually explicit image to send to a boyfriend or girlfriend, which was then shared with another person.



Twenty-eight of 33 responding members indicated they have encountered offenders who have used extortion, blackmail, threats, and other forms of coercion to induce victims into producing child pornography images. Twenty-three members saw an increase in the number of cases involving extortion in the past five years. For example, one country described “severe cases in the use of blackmail, whereby victims are forced into generating indecent images of themselves for the offender” and noted that “there have been a number of victims who have self-harmed as a result and, tragically, some have taken their own lives.”



Responding countries have found that investigations of child pornography trafficking offenses have discovered additional information relevant to the sexual exploitation of children. Twenty-two of 33 countries reported that law enforcement officers had uncovered previously undisclosed child sexual abuse contact offenses during these investigations. Twenty-one of 29 responding countries reported that they encountered offenders who had a prior conviction for a child sexual abuse contact offense during these investigations.



“More abuse, percentage wise, seem to be documented now and will often be found on the phone/on computers belonging to the suspect. One of our problems is that the unknown and new images ‘drown’ in the very large numbers of other and non-self-produced number of images/films/files - making finding them more difficult without good tools/quality hash lists.”

“More offenders with prior conviction are anticipated, and statistics demonstrate that the number of second and third-time repeat offenders is on the rise. Offenders learn from experience (previous disclosure and police techniques that caught them). Offenders evolve to utilize methods to avoid detection, for example using public Wi-Fi, encryption, etc.”

“It [has been] observed that . . . the majority of child pornography offenders [are] committing [child] sexual abuse offenses.”

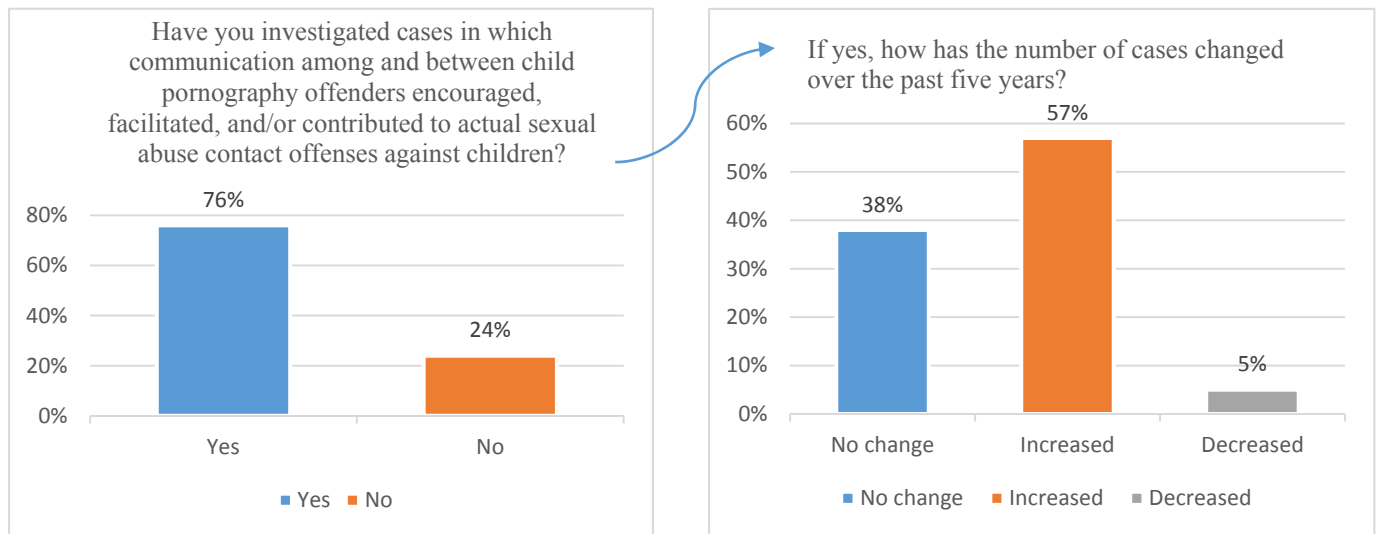
“There is a greater propensity to be a physical offender if the individual is also a collector of child sexual abuse images.”

These responses demonstrate that the threat to children posed by online sexual offenders is increasing. Offenders are seeking more extreme materials, and they are seeking materials depicting younger victims. Self-production by children is increasing due to factors such as social pressure, sextortion, and/or blackmail. The volume of pornographic material continues to increase as encryption and anonymization techniques improve. Many countries expect that the number of offenders will increase and, as internet capabilities improve around the world, the volume of child pornography will increase.

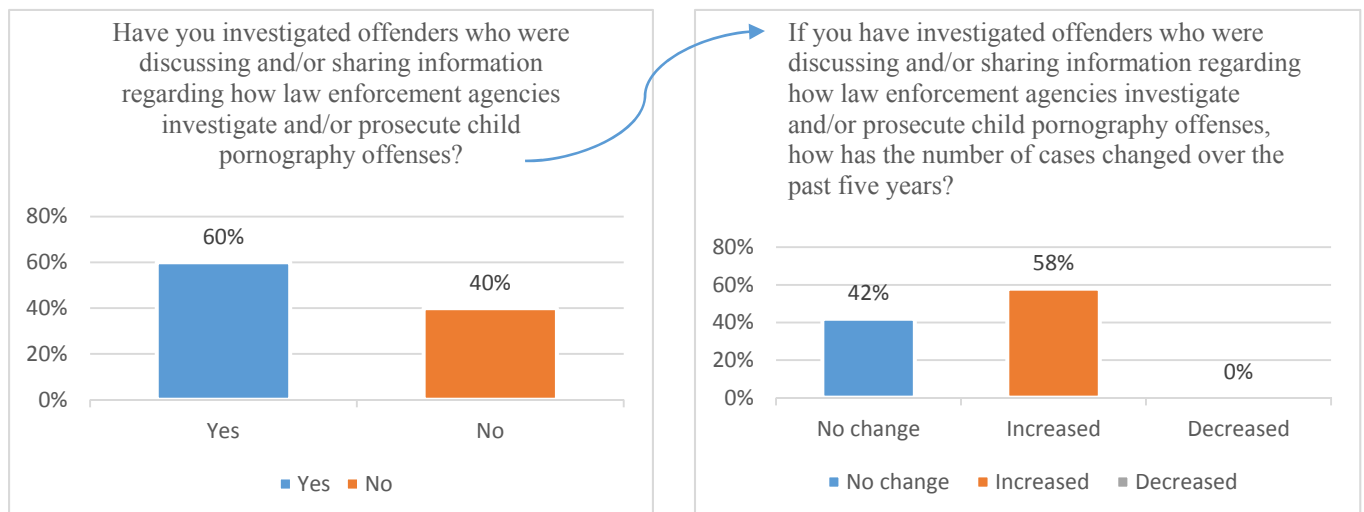
Communications Between Child Pornography Offenders

One of the more serious problems facing reporting countries is the ease with which offenders are able to use online forums, peer-to-peer exchanges, social media, and anonymous networks to communicate with other offenders and thereby facilitate internet child sexual abuse offenses. This section addresses some of the challenges and consequences that countries face when offenders communicate with each other.

Communications between offenders encouraging or facilitating sexual contact offenses against children have dire consequences. For example, 22 of 29 responding countries have investigated cases where communication between offenders encouraged and/or contributed to actual sexual abuse offenses against children; 12 of 21 countries reported that the number of such cases has increased over the past five years.



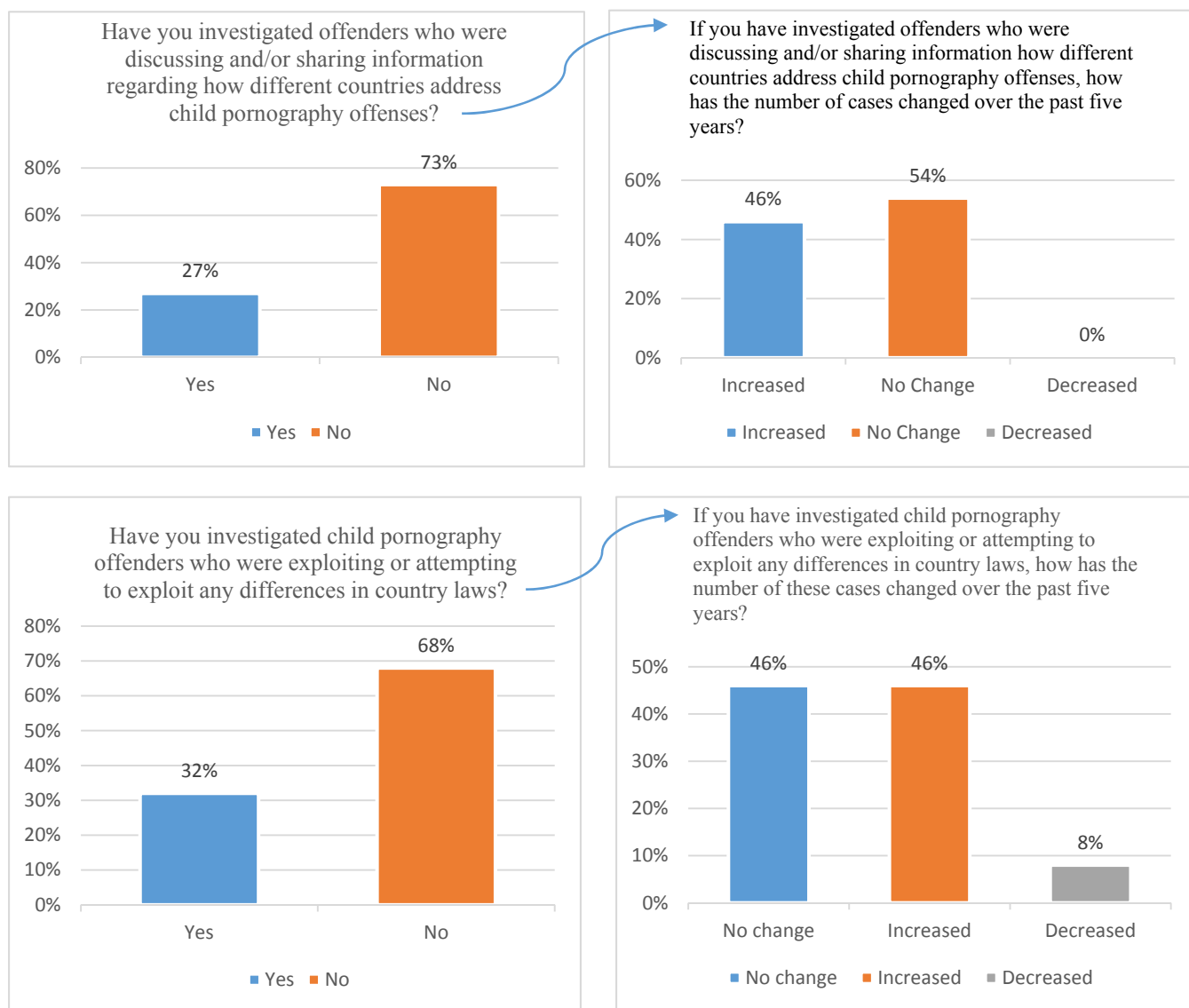
Additionally, 18 of 30 responding countries have investigated offenders who were discussing and/or sharing information about how law enforcement agencies investigate and/or prosecute child pornography offenses. Eleven of 19 responding countries indicated this has increased over the past five years. Offenders are increasingly educating each other on how to use private chats, email, internet voice and video chat software, forums, and anonymization software.



“Individuals chatting in [an anonymous network] have been observed to be encouraging others to sexually abuse children they have access to and upload that content. To demonstrate that these are new images/videos the offender is sometimes requested to put a personal signature on their image such as they get the child to hold up a piece of paper stating their name and the date to prove the image is live and original.”

“Offenders are using tutorials [on] how to avoid on site investigations or how to avoid being arrested and [prosecuted]. These tutorials are distributed among offenders with the use of private chats, mails, [internet voice and video chat software,] forums and anonymity networks.”

Responding members have found that offenders are discussing and exploiting the differences in child pornography laws around the world. Eight of the 30 responding members investigated offenders who were sharing information regarding how different countries address child pornography offenses; 6 of 13 reporting members indicated that there has been an increase in the number of such cases over the past five years. Nine of 28 reporting members investigated offenders who were exploiting or were attempting to exploit different countries’ child exploitation laws. Six of 13 responding countries saw an increase in the number of these cases over the past five years.



* * * *

The responses in this section emphasized that new technology is making it easier for child sex offenders to communicate online in order to facilitate the sexual abuse of children in various ways. Offenders are providing one another with tutorials on grooming and enticing children. Offenders encourage each other to utilize encryption and anonymization to avoid law enforcement. Offenders track and disseminate information regarding law enforcement's technologies, techniques, and tools for combating the sexual abuse of children. Offenders also are trading information about: (1) which countries can be visited most cheaply; (2) which countries have police and courts that are corrupt and/or willing to accept bribes; and (3) those countries where the perceived risk of detection is lowest.

“It becomes more and more common that offenders inform each other about [their] activities, especially when there is special bulletin board dedicated to these individuals: in such case there is almost always special website which focuses only on [security] matters and provide information regarding to how to avoid detection and identification by [law enforcement agents].”

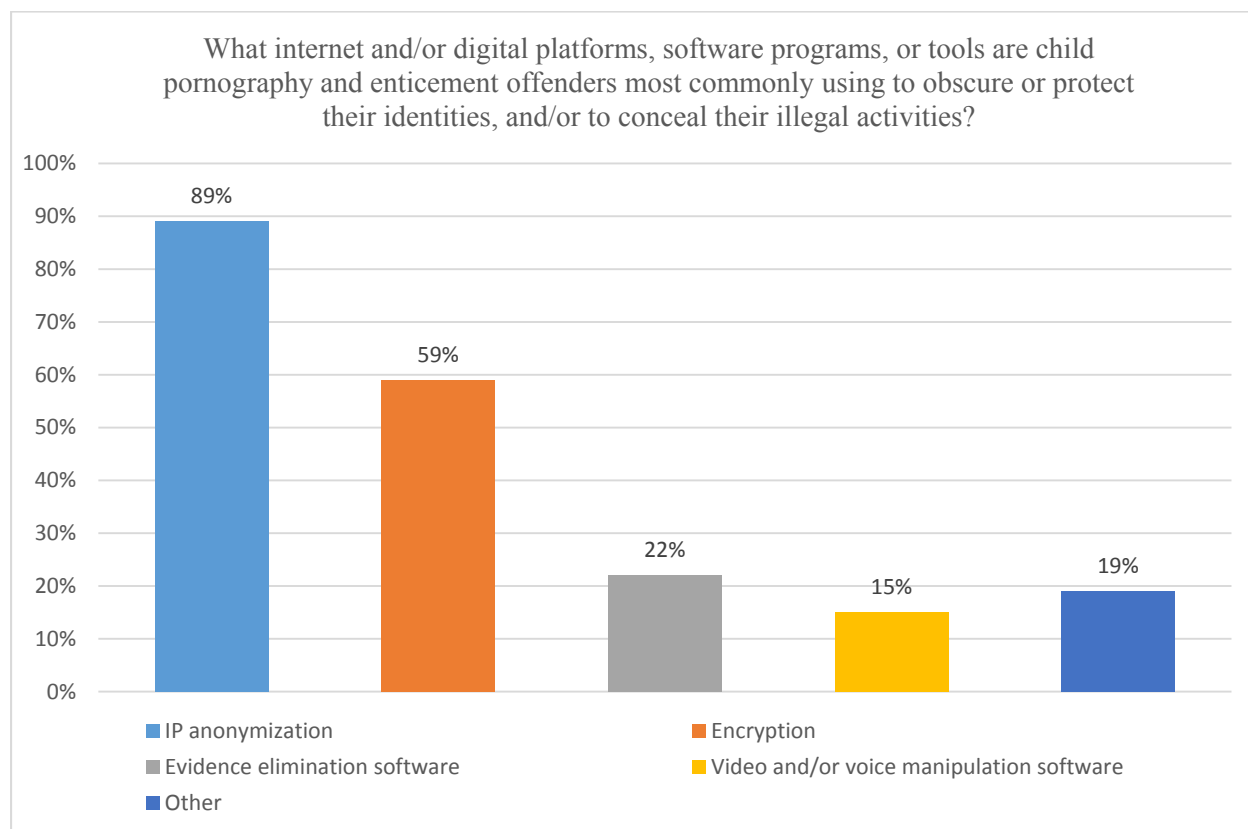
“Many websites have been recently observed where offenders readily post images of their children and encourage comments and feedback from their peers/like-minded individuals. Such comments may encourage sexual abuse. The number of cases has increased, however, many sites can be hard to locate/infiltrate.”

“Offenders [are] seeking more extreme materials, and materials depicting younger victims, from one another[.] Provision by offenders of tutorials to other offenders regarding how to groom and entice minor victims, especially online [p]roduction on demand: offenders can ask another offender to perform specific sex acts with a child”

Technological Issues & Challenges Faced by Law Enforcement

With the continuing development of technology that offenders can use to commit child sexual offenses online, countries are experiencing even more limitations and challenges that negatively impact their investigations into these offenses.

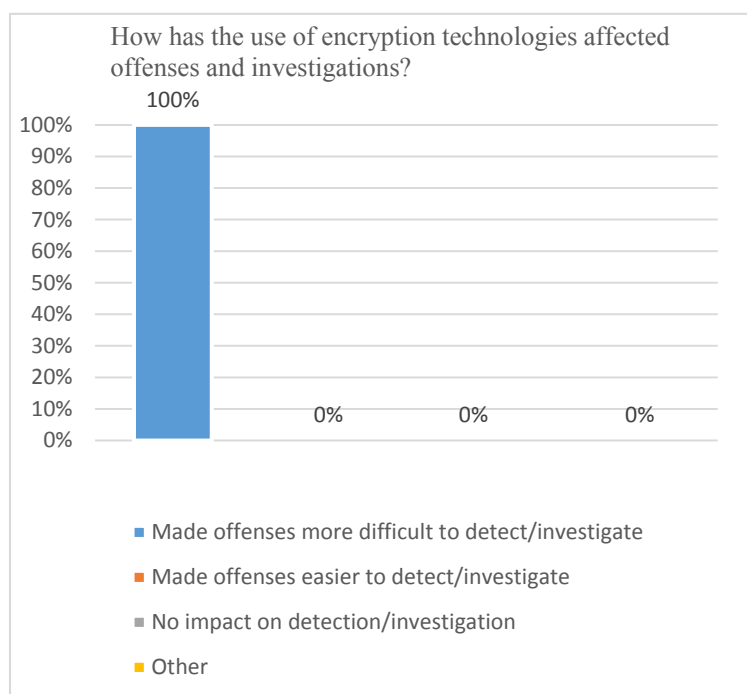
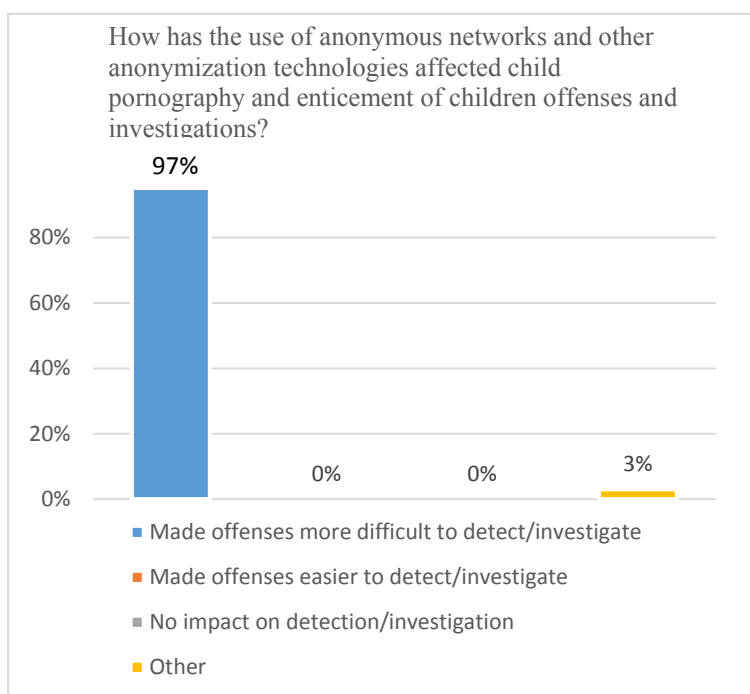
For example, offenders are using internet and/or digital platforms, software programs, and other tools to obscure or protect their identities, and/or to conceal their illegal activities. Twenty-four of 27 reporting members identified Internet Protocol (IP) address anonymization as the most commonly used means by which child pornography and enticement offenders cover their tracks. Sixteen reporting members indicated encryption, 6 listed evidence elimination software, and 4 identified video and/or voice manipulation software as ways that offenders have attempted to protect themselves and conceal their illegal activities. Such methods have increased recently, as 23 of 27 responding countries saw an increase in offenders utilizing these technologies in the past five years.



“There has been a slight increase in the use of software facilitating anonymity, and the availability of this technology. Devices will be made with built-in encryption requiring no user intervention, and the use of such technology will become easier, even for the less technically-inclined users. More offenders will be using these methods to conceal their identities/avoid detection, and will share these methods with other offenders.”

These tools are hindering law enforcement investigations into internet child sexual abuse. Twenty-eight of 29 responding members revealed that the use of anonymous networks and other anonymization technologies made child pornography and enticement of children offenses more difficult to detect and investigate.

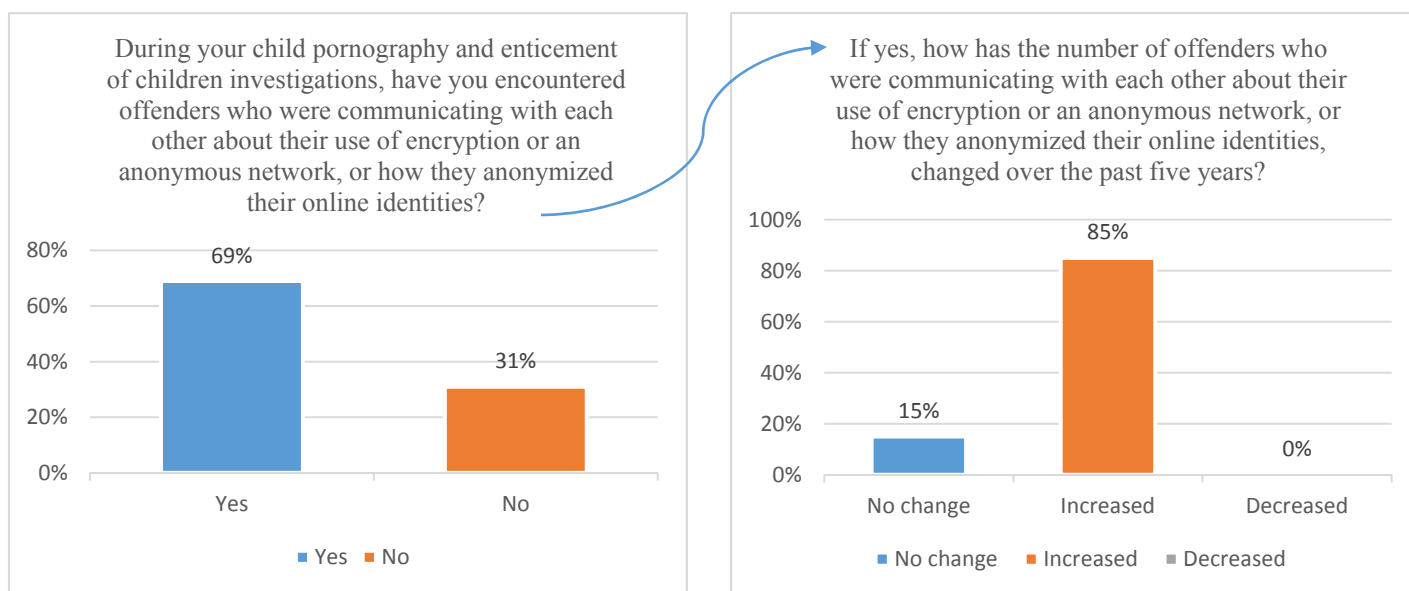
One country reported that “it is becoming easier and easier for potential perpetrators to use high tech security protocols in order to obscure their identity. This is the result of very user friendly software that allows people with very limited digital knowledge to make use of [an anonymous network].” Anonymization software makes it difficult to locate offenders because their computer is hidden. Encryption can rarely be broken through brute force; the password is typically required. All 27 responding countries identified the use of encryption technologies as hindrances to investigations. It is evident that offenders are using technological methods to evade detection and such actions have made investigations more difficult around the world.



“As offenders are becoming more familiar with this technology, more are using it. . . . [T]he more awareness/concern for privacy, the more the technology will advance/protect online activities. It will be easier for everyone to have the ability to use these detection avoidance techniques, even those who are not tech savvy, and devices will be made with built-in encryption requiring no user intervention. Encryption is more complex, and is more involved and difficult to get through. When data is encrypted, there is a reliance on the suspect, as s/he must provide the password.”

* * * *

Not only have offenders been utilizing encryption and anonymous networks, they have been communicating and sharing their techniques with each other. Twenty of 29 reporting members encountered offenders who were communicating with each other about their use of encryption or an anonymous network, or how they anonymize their online identities. Of the 20 responding countries, 17 saw increases in such cases. The increased use of these technologies as well as the sharing of criminal tradecraft is creating even more challenges for law enforcement in identifying these offenders.



“We have observed that most of the offenders that communicate with others have two main questions which are where to find new material and how to hide the material they already have. We anticipate that the number of the offenders who will know how to use proxies and encryption will increase.”

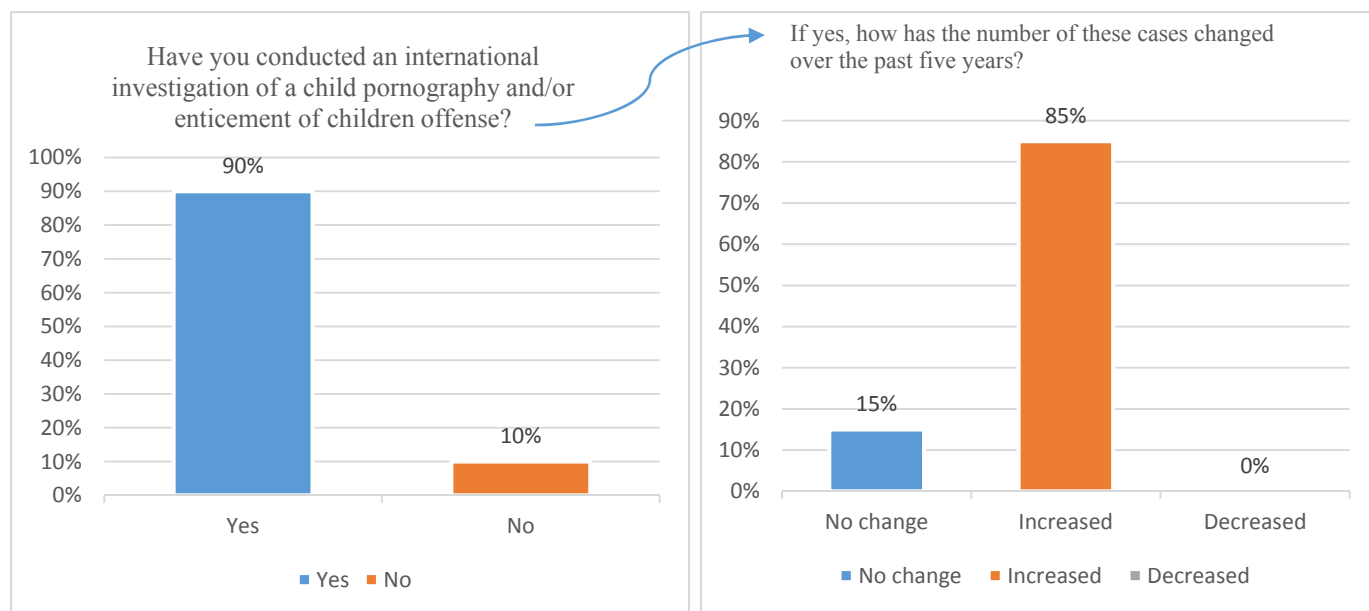
International Legal Issues and Challenges

With new technology making it easier for internet child sexual abuse offenders to commit crimes across borders, more and more countries are conducting international investigations into child pornography and/or the enticement of children. The term “international investigations” was defined in the threat assessment questionnaire as investigations in which offenders, victims, witnesses, or evidence are located in more than one country. Many countries reported that international investigations of child pornography and enticement pose a unique set of challenges.

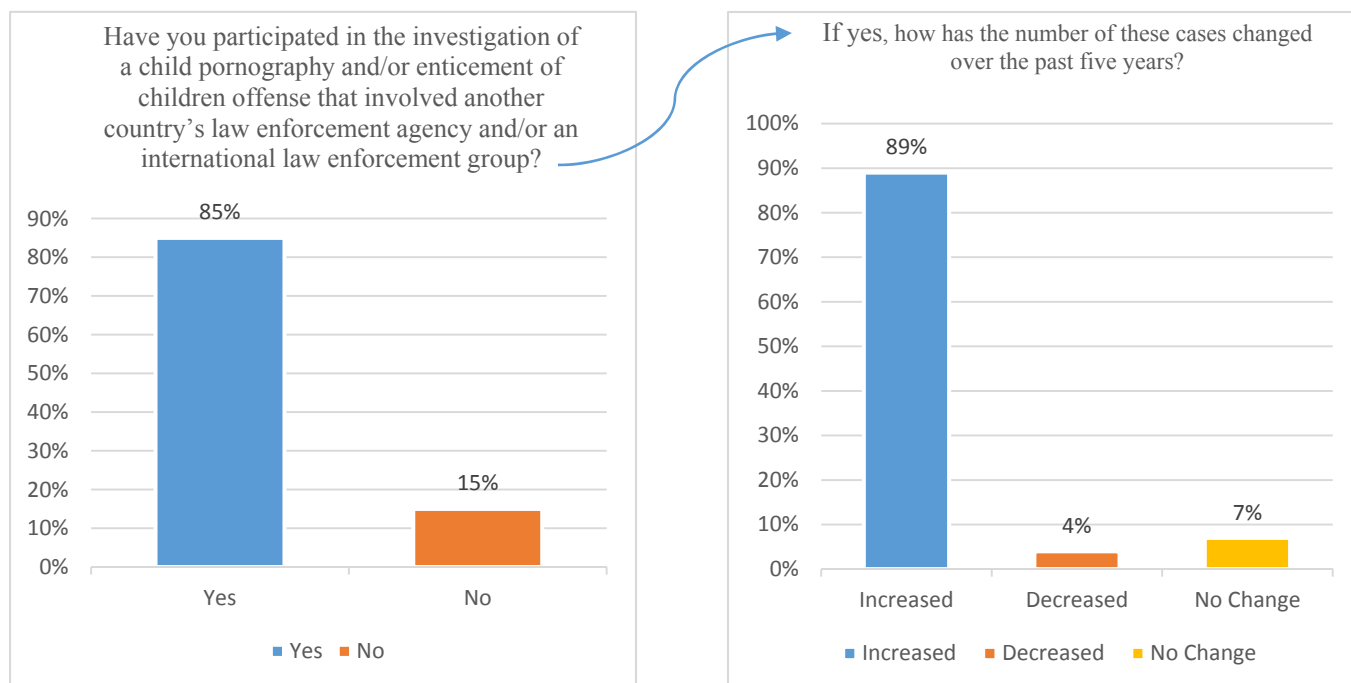
Twenty-seven of 30 responding countries reported that they had conducted an international investigation of a child pornography and/or enticement of children offense, with 22 of 26 reporting that the number of these international investigations has increased in the past five years.

Due to the global nature of many of the crimes involving child pornography and/or enticement of children, there are often overlaps in investigative and legal jurisdictions. Twenty-nine of 34 responding countries participated in investigations of child pornography and/or enticement of children offenses that involved another country’s law enforcement agency and/or an international law enforcement group (*e.g.*, INTERPOL, Europol). Twenty-five of 28 countries that participated in these investigations saw an increase in the number of these cases over the past five years.

Many countries reported that the international scope of many investigations has made them more challenging because there are jurisdictional obstacles to obtaining evidence. Obstacles include no unified thresholds for illegal conduct and delays in obtaining important evidence. For example, one country explained that “due to international aspect and the long duration of the execution of an international warrant, it is difficult to get the needed information in a reasonable time-frame.”



“With the use of internet, more and more cases have international characteristics. The offenders not only collect such material but they use the internet in order to distribute it too. In most case[s] the distribution that takes place involves more than one country. We anticipate that most of the case[s] in the near future will have to be addressed in an international manner with the coordination of Interpol and Europol.”



“Offenders are getting more and more familiar with the using of Internet, [peer-to-peer] networks, etc. It means that they get in connection with foreign offenders, foreign websites, chat rooms, storages. This all indicates that international law enforcement cooperation has to also increase. Another relevant reason is that more and more law enforcement authorities make their own peer-to-peer investigations which generate a large amount of criminal information which they send out through the world. Due to this kind of information more and more national investigations will be started with international links. And the whole cycle starts again.”

The responses in this section underscore the challenges international investigations into internet child sexual offenses raise for law enforcement. Offenders' commission of transborder crimes make it difficult for law enforcement to investigate. The international scope of investigations requires international cooperation where laws and procedures often differ. Many responding countries complained that the many variances in the laws of other countries cause routine and frustrating delays.

Conclusion

As the data collected in this threat assessment confirms, online child sexual abuse offenses are evolving and becoming more prevalent, more extreme, more complex, and more difficult for law enforcement agencies to investigate. Even as countries undertake steps to strengthen their efforts to prevent and prosecute these crimes, it is evident that the threat to children online remains a pervasive and increasing problem.

Offenders have taken advantage of technological advances in order to avoid detection. Using encryption and anonymization software, offenders are masking their identities and making it difficult for Global Alliance members to find them. More of the most serious and sophisticated offenders are migrating to anonymous networks. Furthermore, offenders are increasingly using technology to communicate with other offenders in order to exchange techniques for evading law enforcement and facilitating the sexual abuse of children online, to share sexual fantasies regarding children, and to trade child pornography. All of this is made even easier through innovations in mobile technology, through which predators are finding more opportunities to entice children.

The volume of child pornography has increased, as has the number of offenders. These offenders will also often use blackmail and extortion to receive more child pornography. Technological advances have also increased children's self-production of child pornography.

The exploitation of children as well as the production and distribution of child pornography has entered international networks. Offenders engage with children and with other offenders from across the globe. While cooperation amongst countries is increasing, many barriers still exist. As offenders are communicating more easily through peer-to-peer networks, forums, and social networking sites, international investigations are often slowed by ineffective communication, difficulty in obtaining evidence, and constraints imposed by differences in laws.

The challenges identified and evaluated in this threat assessment underscore the importance of cooperation and collaboration between Global Alliance members as well as other countries in combating online child sexual exploitation. Through collective international action, the Global Alliance's four policy targets can be achieved.