GDPO Working Paper Series

Working Paper No.6 (April 2020)

Seoul Searching: South Korea's AI Counter-Cryptomarket Capability and Associated Privacy Dilemmas

Martin Horton-Eddison*

Key Points:

- Working paper uses translated sources to provide a Korean view of Drug Cryptomarkets
- Highlights ROK drug policy as linked to broader geopolitical considerations
- Identifies policy linkage between Child Pornography and Drug Cryptomarkets
- Examines Republic of Korea's use of advanced proprietary AI software to crawl the deep web for signs of drug cryptomarkets – technology not hitherto available to Western enforcement
- Focuses attention on the recent technology for data partnership between a private ROK company and Interpol
- Raises questions around the ethics of private-public data sharing, accountability of investigation methods, transparency, and international jurisdiction
- Notes that the continued absence of a UN cybercrime treaty with specific provision for drug cryptomarkets leaves enforcement and the private sector to operate without policy oversight at the international level
- Accompanying video: https://tinyurl.com/GDPOtube

* Drug Cryptomarket Project, Global Drug Policy Observatory & Lecturer of International Relations, Cardiff University

Introduction:

Despite recent increases in Russian and Chinese markets[1] and vendors, much analysis of Drug Cryptomarket[†] (DCM) policy and enforcement operations has been largely focused on English language markets either located in, or serving, buyers in North West Europe, North America, and Australasia. However, the Republic of Korea (ROK) has been quietly developing – in conjunction with domestic academic and corporate partners – highly sophisticated counter-crypto capabilities. By March 2020, ROK technologies were so advanced that Seoul-based *S2W Lab* were invited to enter a technology-for-data partnership with Interpol. The year-long arrangement formalised mass data sharing between the ostensibly private organisation and international law enforcement. How – and why – the Republic of Korea has moved so far forward in counter-crypto enforcement capabilities is worthy of attention.

> ***'We show best practices regarding monitoring of selling and trafficking of drugs on the internet…since 2016, we have been operating an internet monitoring system which is able to automatically search for any possible trace of drug trafficking on the internet around the clock'***
>
> Yongsoo Lee, Deputy Permanent Representative of the Republic of Korea to the United Nations, Plenary Statement at Opening of the 61st Session of the Commission on Narcotic Drugs, Vienna, 12th March, 2018

This brief utilises qualitative analysis of translated open source Korean-language information, political statements, and news sources to detail ROK's drug laws to bring closer attention on this understudied regional player. The analysis is framed by an introduction to ROK's most recent Narcotics Control Act (2016), within the context of Korea's membership of relevant international organisations and regional groupings. It also provides information on Korean use of drug cryptomarkets (DCMs), identifying the policy linkage between DCMs, financial crimes, and child pornography. The paper also provides a comprehensive overview of ROK's counter-crypto capabilities, including detailing the new relationship between Korea's private cyber-security sector and Interpol.

Exemplified by S2W Lab's formal relationship with Interpol, the final analysis posits that the integration of private AI-driven processing with public law enforcement data might indicate how broader global counter-DCM operations might evolve in the future. However, the analysis also identifies several possible issues for concern around such an approach, including but not limited to; ethical considerations around private-public data sharing, accountability of investigation methods, transparency, and international jurisdiction. South Korea's contestable view of personal privacy – coupled to particularly stringent anti-drug laws – risks establishing new enforcement norms counter to the increasingly progressive attitudes in some other states.

Attitudes, Legislation, & Response

Despite ROK's relatively recent ratification of the three international drug treaties (2007), Korea has a long domestic history of legislating against the non-medical use of drugs and has some of the most punitive drug laws in the world. South Korean attitudes to drugs are rooted in conceptions of drug use as synonymous with the threat from the North, indeed drug use in South Korea has been inextricably linked with the broader geo-political picture since the 1950s. In the 1970s, amid the zenith of the Cold War and ongoing tensions on the Korean peninsula, cannabis in particular[‡] became subject to strict government control in 1976. Considered a symbol of the left-leaning American counter-cultural movement and a dangerous threat to South Korean sensibilities, the Cannabis Control Act of 1976 (CCA76) indelibly tied recreational drug use to considerations of national security. Launched at the same time, publicly funded

[†] Also known as Darknet Markets, Crypto Drug Markets (CDMs),
[‡] Republic of South Korea, Cannabis Control Act, 1976

propaganda films underscored the implication of cannabis in the broader Left-Right ideological struggle at the heart of the South's relationship with the North. Justifying CCA76, then President Park Chung-hee[§] decreed that South Korea 'must pull up by the roots the problem of marijuana smoking and similar activities'[2] to be achieved by applying 'the maximum penalties currently available under the law.'[3] Launched in South Korea's own dictatorial era, CCA76 set the tone for the next four decades of legislative and ongoing social attitudes.

Today, the most recent revision (2016) of the Narcotics Control Act (2000) draws together CCA76's focus on cannabis with Opium[**] (1957), Methadone and Barbituates[††] (1970), and Methamphetamine, Glue, and Butane[‡‡] (1980) with little distinction in enforcement and penal terms. According to NCA2016, there is no distinction in enforcement or sentencing between 'soft' drugs such as cannabis or MDMA, or problematic drugs including crystal methamphetamine, and heroin. Indeed, the use or possession of cannabis – or just the seeds or husks - can result in prison sentences of up to five years, or fines as high as ₩50million KRW (~$40,000USD). Moreover, Korean police can – and frequently do - stop and forcibly hair follicle test anybody on public streets for the use of drugs. Providing a positive blood sample for cannabis[§§] - even if consumed abroad and in a jurisdiction with legally regulated cannabis markets before flying to Korea - is considered the same as physical possession. Korean citizens face the full force of the law, and foreign nationals can expect to be deported.

One consequence of this approach is to directly impact the risk/reward quotient for those intent on supply. Indeed, anecdotal evidence[4] suggests cannabis sells on the streets of Seoul at between $100-200 a gram, with cannabis resin obtaining twice as much. LSD costs $200 per tab, and methamphetamine as much as $1000 per gram. Korean street prices are therefore higher in all categories compared with prices in the Anglosphere and Europe, confirming Korea's strictly punitive approach acts as a significant price catalyst.

Cryptomarkets as Response to Punitive Approach

At the same time, South Korean society has a cultural propensity for embracing new technologies, including developing the first online microtransactions in 1996, and social networking in 1999. Since the 1990s, South Korea has also been the world leader in the invention and adoption of broadband and wireless technologies. This is also true of cryptocurrencies; by 2017, ROK was the world's third largest market for Bitcoin, and the largest market for Ether.[5] Indeed, although South Korea has less than 1 percent of the world's population, estimates indicate it is responsible for 30 percent of all global cryptocurrency trades by value.[6] Korea has also been quick to adopt the technologies behind cryptocurrencies, most notably blockchain; Korean manufacturing giants Hyundai Motors and Samsung have both integrated blockchain into the core of their businesses.[7] At the same time as placing a societal premium on advanced technologies, ROK also has a highly computer-literate population. Perhaps unsurprisingly given the legally and socially prohibitive nature of Korean drug laws, some users and vendors have therefore turned to the technical (and anonymous) nature of drug cryptomarkets – and cryptocurrencies - to evade deeply conservative criminal and societal sanctions, and concordant high street prices.

As far back as 2015, officials of the International Investigation team of the Korean Customs Service noted a spike in the number of postal packages containing drugs arriving from North America and Europe. Closer investigation revealed that individual users were cutting out Korean street dealers – and the associated risks – by purchasing drugs directly from foreign websites.[8] In response, Korean Customs constructed and despatched a dedicated drug detection team to

[§] Dictatorial South Korean President, 1963-1979
[**] South Korea, Narcotics Act, 1957
[††] South Korea, Act on Habit-Forming Medicine, 1970
[‡‡] South Korea,Toxic Chemicals Control Act, 1980
[§§] Korea's maximum penalty for a positive follicle test for cannabis is five years custodial sentence

Incheon International Airport to specifically target international mail packages carrying drugs bought online.[9] South Korea recorded its first drug cryptomarkets-related arrest in the same year; a 27year old Seoul resident was apprehended for using cryptomarkets to import drugs for personal use, and for distribution to international students studying in the country.[10] Within a year, the use of drug cryptomarkets to import substances had grown exponentially. By February 2017, Korea's National Police Agency reported to law makers that they had found over 50,000 Korean language posts on cryptomarkets[11] advertising not just drugs, but a plethora of illegal materials including child pornography, and carding information, on a range of Korean language cryptomarkets.

Echoing historic framing of cannabis as analogous to peninsula rivalries, drug use remains perceived as indelibly linked to the North. This is particularly true of crystal methamphetamine, driven by reports of state-sponsored use of p*ingdu* (crystal methamphetamine) as an appetite suppressant and to boost productivity in the DPRK.[12] A secondary factor is that it isn't just the South that has embraced cryptocurrencies; at the State level, North Korea is also invested. Desperate for hard cash due to international sanctions, DPRK sees accruing cryptocurrency as a way to circumnavigate international trading restrictions.[13] There is growing evidence that North Korea's state-sanctioned crystal methamphetamine production programme is also designed to generate currency by finding its way onto international markets.[14] In China, DPRK *pingdu* is considered high quality, and makes its way onto cryptomarkets via Chinese vendors importing directly from the DPRK and selling online. However, there is as yet no evidence of North Korea selling illegal drugs *directly* on drug cryptomarkets.[15]

Taken in the round, South Korean law makers have decried cryptomarkets as a threat to ROK national security. Representative Song Hee-kgyoung of Korea's legislature noted 'worsening' of the problem and declared South Korea 'practically defenceless against these crimes.'[16] She noted the issue was 'international', and urged the Korean government to work toward enforcement solutions. By 2019, Son Young-dong, professor of convergence and defence at Hanyang University, added to the securitization narrative, declaring 'the Dark Web is a great threat to [South] Korean society.'[17]

In response, ROK made specific provision in the Republic's new NCA2016[18] to include jail terms for dealing or buying drugs online. Subsequent increases in enforcement measures resulted in 80 Korean residents arrested for buying or selling drugs on cryptomarkets in 2016, with a further 75 arrests in 2017.[19] In late December 2018, South Korean law enforcement apprehended one market administrator and 8 vendors for using a drug cryptomarket to distribute illegal drugs enabled by the internet.[20] Although a small site by comparison to English language services,[21] (636 members) this was nevertheless significant as it marked the first time in Korea that a market administrator of a Korean-language drug cryptomarkets had been arrested and the website closed down. Korean prosecutors alleged that the marketplace had been established in order to sell *Pingdu*, as well as psychoactive substances, including LSD and MDMA, imported online from 'neighbouring countries'[22] in order to retail on the Korean language site. Investigations showed that the suspects had completed $88,000 of transactions using cryptocurrencies including Dash (DASH) and/or other cryptocurrency including Monero (XMR).[23] All nine of the arrests were also formally charged with 'smoking marijuana' under the provisions of NCA2016.

ROK Capabilities

ROK's broader crypto policy intersects with these broader geopolitical concerns, and focusses on two specific issue areas: financial fraud including money laundering, and the use of crypto technologies to monetise and distribute child pornography. Tacked on to this, drugs appear as an undistinguishable feature of far broader considerations.

Despite the securitisation rhetoric and some limited enforcement successes, until late 2019 the entirety of Korea's dark web cybercrime enforcement effort consisted of a six-member task force based within the National Police Agency (NPA). Since November 2019, the NPA team has been augmented by regional 'cyber investigation squads' located at district police agencies throughout the country,[24] as well as other state entities including the International

Investigation team at the Korea Customs Service**.** Domestic efforts are augmented by international relationships including with UK and the United States: In March 2018, as a result of joint counter-darknet enforcement operations involving South Korean National Police, the UK National Crime Agency (NCA), and US federal agents, Jong Woo Son, 23, a South Korean national, was arrested for his operation of *Welcome To Video,* the largest child sexual exploitation market by volume of content on the darknet.[25] Based in South Korea, the server location, administrator, and an additional 337 site users (of whom 223 where South Korean nationals)[26] were identified through the 'sophisticated tracing of bitcoin transactions.'[27] The same tools employed in this operation appear to be those revealed by Yongsoo Lee's 2018 revelation[28] that ROK operates an internet monitoring system to automatically search for any possible trace of drug trafficking on the internet around the clock**.**

The Tools

In 2020, ROK law enforcement employs technically sophisticated Artificial Intelligence (AI) programmes developed by South Korea's *S2W Lab*, a data intelligence company established in September 2018. S2W Lab's source of funding is opaque, but given the nature of its work, and its ties to the state-owned Korean Advanced Institute of Science and Technology University (KAIST), it is highly likely that it is (in)directly funded by the South Korean government. Indeed, S2W Lab's analytical tools have been developed alongside academic research from KAIST; researchers conducted a number of scientific studies on machine learning on the 'dark web', published in peer reviewed academic journals. A significant number of those researchers[***] also occupy senior roles in S2W Lab, applying the results and methodologies to assist in developing a number of proprietary software tools for counter-crypto operations.[†††]

S2WLab's mission is to 'prevent the adverse effects of anonymity networks and cryptocurrencies to provide [a] healthier and safer cyberspace.'[29] S2W Lab exists to collect and build a massive 'dark web' database, and analyze it with an artificial intelligence (AI) engine. It also employs automated natural language processing (NLP) techniques to search for links between drug market listings to cross reference vendors across distinct time periods and domains. The Lab's software covers both cryptocurrency transaction history and general web data in the dark web and is thus applicable to a range of crypto-related tasks. S2W Lab's software examines data crawled from the darknet to establish links among multiple domains and among multiple timeframes. The company has secured several patents on its software, including *S2-Xarvis* and *S2-Eyez*.

S2-Xarvis

S2-Xarvis, is S2W Lab's patented multi-domain cross-analysis solution, employing AI to assist in passive tracking and active crawling of the darknet for 'malicious' website coding, and specific images (such as product listings or child pornography). The tool therefore allows for searching of known and novel drug cryptomarkets. Further, S2-Xarvis' AI functionality can be pointed at specific sites to monitor changes to the site's source code, new user registrations, specific product listings. Moreover, NLP analysis of text snippets allows S2W Lab to identify users across multiple platforms. S2WLab also claims S2-Xarvis is capable of cross-analysis of multiple sources of information simultaneously, generating intelligence on cryptocurrency transaction history across space, jurisdiction, and time. For example, in March 2020 S2W Labs' software rapidly identified the formation of a black market for face masks on cryptomarkets. By analysing the prevalence of keywords pertinent to coronavirus across popular darknet markets, S2W Labs were able to locate listings for face masks (selling for between $85 and $170) on cryptomarkets. S2-Xarvis can be directed – and makes no ethical or moral distinction between – a number of crypto threats.

[***] For example: S2WLab's Chief Technical Officer (CTO), Shin Seungwon, is also Professor of network research at the Korean government established *Korean Advanced Institute of Science and Technology* (KAIST)

[†††] Shin co-authored KAIST's Changhoon Yan, Kwanwoo Kim, Yongdale Kim, Seungwon Shin, & Sooel Son, *Doppelgängers on the Dark Web: A Large-scale Assessment on Phishing Hidden Web Services*, WWW'19, The World Wide Web Conference, May 2019. Pp. 2225-2235

S2-Eyez

SW2 Lab's patented *S2-Eyez*[30] – an anti-money laundering solution - allows users to check whether they are conducting cryptocurrency transactions to or from 'known threat actors'[31] such as 'drug traffickers, scammers, or terrorists.'[32] S2-Eyez works by tracing crypto transfers across multiple domains and multiple timeframes - cross referencing with a second AI-constructed 'detection engine' that predicts the 'illicitness' of specific cryptocurrency addresses. [33] S2-Eyez allows Korean law enforcement agencies to trace, observe, and enforce against hitherto difficult to trace cryptocurrency transactions. Once again, S2-Eyez treats malicious transactions associated with child pornography and money laundering in the same manner as drug cryptomarkets without inbuilt distinction, leaving law enforcement to draw such distinctions (or otherwise).

Interpol involvement

Summarily, via S2W Lab, ROK has technological capabilities far in advance of those available to Western enforcement agencies. In less than three years, S2WLab's CEO Sanduk Suh[34] claims to have found more than 10 million cryptocurrency accounts using the company's proprietary software, allowing the company to report accounts suspected of being involved with illegal activities to be investigated by Virtual Currency Exchanges (VCEs). VCEs, working to remain in compliance with domestic Korean anti-money laundering regulations (constructed in compliance with UN conventions[‡‡‡]) are then able to investigate deposit and withdrawal transaction details and pre-block or 'black list' of specific accounts.[35] Such technologies allow Korean VCEs to prevent money laundering, and vendors from 'cashing out' cryptocurrencies into *fiat* currency. Taken together, *S2 Eyez* and *S2-Xarvis* are also very attractive to those seeking to enforce against crypto-facilitated cybercrime across international jurisdiction. Indeed, following successful participation[36] at an Interpol World event in 2019, S2W Lab concluded an agreement in March 2020 to provide services to Interpol, free of charge for a year. The agreement was made possible by integration: S2WLab's Chief Technical Officer (CTO) and KAIST Professor Shin Seung-won is also a member of Interpol's *Global Cryptographic Bank Crime Prevention Subcommittee.* S2W Lab's CEO Sanduk Suh confirmed that the partnership will see S2W Lab 'cooperate with international investigations.'[37] In return for free services, the arrangement commits Interpol to sharing intelligence data with S2W Lab in return for data gleaned by the company's proprietary software.[38] The concept of a law enforcement - private company partnership was pioneered by the Netherlands National High Tech Crime Unit (NHTCU) and Bitdefender's collaboration during Operation Gravesac against Hansa Market in Summer 2017.[39] However, in that instance, Bitdefender *provided* information to law enforcement in order to ensure compliance with domestic regulations: one-way traffic. The nature of the S2W Lab arrangement with Interpol is reciprocal, with no guarantee of enforcement success in return for the sharing of mass data, intelligence information, and (presumably) private identifying information outward from an international agency to an ostensibly private company operating sophisticated AI data processing systems. This may be problematic without appropriate policy direction and / or ethical oversight, especially considering Korea's strategic linkage between a number of related but distinct issue areas.

Conclusion / Analysis

Summarily, the Republic of Korea has developed highly sophisticated AI-driven software for monitoring activity on the cryptographically obscured portion of the internet. However, it has done so through opaque relationships with private companies. Moreover, ROK's particularly punitive drug laws, coupled with engrained social and political conceptions of drugs as somehow analogous to its ongoing conflict with the North require further consideration and should be subject to international policy guidance. Indeed, South Korea is a significant and influential member of UNODC's Heads of National Law Enforcement Agencies, Asia Pacific[§§§] (HONLAP) regional grouping, a Commission on Narcotic Drugs

[‡‡‡] The United Nations Convention Against Corruption (UNCAC) is the only legally binding international anti-corruption multilateral treaty, compliance is managed by the United Nations Office on Drugs and Crime (UNODC)
[§§§§§] HONLEA Asia and the Pacific (HONLAP) was established by ECOSOC Resolution 1845 (LVI) of 1974

(CND)[40] subsidiary body responsible for enabling inter-agency law enforcement cooperation across the Asia Pacific region.[41] In line with broader global counter-crypto strategies, countering illegal money flows using cryptocurrencies is a key focus of the regional counter-crypto strategy, and is the sole focus of HONLAP's expert working group in this arena. HONLAP met in late 2019 to consider joint strategies for countering money-laundering, illicit financial flows and the use of the darknet and cryptocurrencies in relation to the drug trade. HONLAP's expert working group noted that such efforts are inadequately supported by international organisations, and are often ineffective.[42]

Within this frame, ROK has sought to assume a leadership role in HONLAP; it is due to host the upcoming 44th meeting of HONLAP in Seoul, September 2020 to 'discuss control strategies and international coordination on drug problems.'[43] In the absence of effective support and guidance from UN organisations, ROK's increasingly influential position has the potential for its public-private technological approach to influence regional approaches as an example of 'best practice regarding monitoring of selling and trafficking of drugs on the internet.'[44]

More broadly, highly sophisticated and invasive surveillance and monitoring technological capacities developed to counter child pornography and serious financial crimes are now increasingly used to counter the online trade in drugs. Enforcement application of such technologies makes no moral distinction between the trade in recreational drugs and the most injurious substances, nor does it necessarily distinguish between those who trade in child pornography and those who buy drugs online. There is no evidence of ethical oversight or framework guidance on the use of AI to process mass data in this way. In fact, rather than providing guidance on cybercrime through international convention or agreement, the international community – through Interpol – has committed to sharing intelligence of worldwide citizen users with a private South Korean data processing company operating from within a punitive state environment. More broadly, ROK's recent use of S2W Lab's technologies as part of joint operations with the United Kingdom and the United States seems unlikely to end at child pornography. Indeed, the Lab's integration with Interpol might be the first step toward broader adoption of AI-driven data processing technologies by law enforcement worldwide.

The ongoing absence of an international cybercrime convention with specific provisions for drug cryptomarkets, continues to be problematic and this is exemplified by the evolving situation described in this report. At the international policy level, UNODC's reliance on intersecting conventions – namely the Convention on Transnational Organised Crime (UNTOC) and Corruption (UNCAC) to deal with drug cryptomarkets remains inappropriate as it continues to draw the drugs issue together with issues of differing magnitude. That this is now reflected in evolved and sophisticated enforcement tools – without treaty or ethical oversight – should focus minds on the appropriateness – or otherwise – of the ongoing ad-hoc approach in Vienna.

supported by

OPEN SOCIETY FOUNDATIONS

About the Global Drug Policy Observatory

The Global Drug Policy Observatory aims to promote evidence and human rights based drug policy through the comprehensive and rigorous reporting, monitoring and analysis of policy developments at national and international levels. Acting as a platform from which to reach out to and engage with broad and diverse audiences, the initiative aims to help improve the sophistication and horizons of the current policy debate among the media and elite opinion formers as well as within law enforcement and policy making communities. The Observatory engages in a range of research activities that explore not only the dynamics and implications of existing and emerging policy issues, but also the processes behind policy shifts at various levels of governance.

Global Drug Policy Observatory

Research Institute for Arts and Humanities

Room 201 James Callaghan Building

Swansea University

Singleton Park, Swansea SA2 8PP

Tel: +44 (0)1792 604293

www.swansea.ac.uk/gdpo

@gdpo_swan

GdPO Global Drug Policy Observatory

reporting monitoring analysis

[1] Martin Horton-Eddison, *US STOP Law Aims to Tackle Postal Deliveries from Dark Web Drug Sales*, Dark Matter - OSINT Snapshots, Jane's Intelligence Review, Vol.30, No.12, December 2018. Pp.24-25

[2] Quoted in: Jason Strother, *Korea's Forgotten High Times*, Yonhap News Agency, 8th February, 2013. Available: https://en.yna.co.kr/view/AEN20130214003200315 (Accessed: 07/04/2020)

[3] Quoted in: Jason Strother, *Korea's Forgotten High Times*, Yonhap News Agency, 8th February, 2013. Available: https://en.yna.co.kr/view/AEN20130214003200315 (Accessed: 07/04/2020)

[4] Asian Junkie, *[Interview] An Inside Look at Drugs in Korea from a Former Drug Dealer*, Asian Junkie, 7th November, 2019. Available: https://www.asianjunkie.com/2019/07/11/interview-an-inside-look-at-drugs-in-korea-from-a-former-drug-dealer/ (Accessed 12/04/2020)

[5] Bernard Moon, *Why South Korea is 'Crypto Crazy' and what that means for the rest of the world,* Venturebeat, 14th July, 2018. Available: https://venturebeat.com/2018/07/14/why-south-korea-is-crypto-crazy-and-what-that-means-for-the-rest-of-the-world/ (Accessed 15/04/2020)

[6] Bernard Moon, *Why South Korea is 'Crypto Crazy' and what that means for the rest of the world,* Venturebeat, 14th July, 2018. Available: https://venturebeat.com/2018/07/14/why-south-korea-is-crypto-crazy-and-what-that-means-for-the-rest-of-the-world/ (Accessed 15/04/2020)

[7] Bernard Moon, *Why South Korea is 'Crypto Crazy' and what that means for the rest of the world,* Venturebeat, 14th July, 2018. Available: https://venturebeat.com/2018/07/14/why-south-korea-is-crypto-crazy-and-what-that-means-for-the-rest-of-the-world/ (Accessed 15/04/2020)

[8] Official of the International Investigations Team, Korea Customs Service, Cited in: Chung Hye-min, *Drug Smuggling Reaches a Record High in South Korea*, The Korea Observer, 6th February, 2015. Available: https://www.koreaobserver.com/drug-smuggling-reaches-a-record-high-in-south-korea-26160/ (Accessed: 13/04/2020)

[9] *Ibid.* Chung Hye-min, 2015.
[10] JP Buntix, *First South Korean Deep Web Investigation has been Officially Recorded*, Bitcoin News, 28th October, 2016. Available: https://www.livebitcoinnews.com/first-south-korean-deep-web-investigation-officially-recorded/ (Accessed 12/04/2020)
[11] Jo He-rim, *155 Busted for Illegal Drug Trade on 'Dark Web'*, The Korean Herald, 27th September 2017. Available: http://www.koreaherald.com/view.php?ud=20170927000887 (Accessed 10/04/2020)
[12] Sheena Chestnut Greitens, *Illicit*: *North Korea's Evolving Operations to Earn Hard Currency*, Committee for Human Rights in North Korea, 2014
[13] Jason Bloomberg, *the Eigh Most Popular Cryptocurrency Transaction Types are not What you Expect*, Forbes, 19th January, 2019. Available: https://www.forbes.com/sites/jasonbloomberg/2019/01/19/the-eight-most-popular-cryptocurrency-transaction-types-are-not-what-you-expect/ (Accessed: 16/04/2020)
[14] Isaac Fish, *Inside North Korea's Chrystal Meth Trade*, Foreign Policy, 21st November, 2013.
[15] Sheena Chestnut Greitens, *Illicit*: *North Korea's Evolving Operations to Earn Currency*, Committee for Human Rights in North Korea, 2014
[16] Jo He-rim, *155 busted for illegal drug trade on 'dark web'*, The Korea Herald, 27th September, 2017.
[17] '*Dark Web', a Hotbed of Internet Crime… 116,000 Visitors a Day,* Hankyung.com, 29th July, 2019. (Translated from Korean). Available: https://www.hankyung.com/it/article/2019072984951 (Accessed 08/04/2020)
[18] Act 14019, *Narcotics Control Act*, Republic of Korea, 3rd February, 2016.
[19] Jo He-rim, *155 busted for illegal drug trade on 'dark web'*, The Korea Herald, 27th September, 2017.
[20] Park Ju-Young, *9 Darknet Dealers Caught for Selling Narcotics with Crypto*, The Korea Herald, 23rd December, 2018. Available: http://www.koreaherald.com/view.php?ud=20181223000103 (Accessed 10/04/2020)
[21] Seoul prosecutors allege that site had 636 members between March and November 2018, facilitating sales of drugs on 50 occasions
[22] Omar Faridi, *South Korea: Authorities Arrest Nine for Allegedly Selling Drugs for Crypto*, CryptoGlobe, 26th December, 2018. Available: https://www.cryptoglobe.com/latest/2018/12/south-korean-authorities-arrest-nine-residents-for-allegedly-selling-drugs-using-cryptocurrencies/ (Accessed: 16/04/2020)
[23] Omar Faridi, *South Korea: Authorities Arrest Nine for Allegedly Selling Drugs for Crypto*, CryptoGlobe, 26th December, 2018. Available: https://www.cryptoglobe.com/latest/2018/12/south-korean-authorities-arrest-nine-residents-for-allegedly-selling-drugs-using-cryptocurrencies/ (Accessed: 16/04/2020)
[24] Kim Arin, *Police Open Full-Scale Probe into 'Dark Web'*, The Korean Herald, 10th November, 2019. Available: http://www.koreaherald.com/view.php?ud=20191110000163 (Accessed 12/04/2020)
[25] United States Department of Justice, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin*, Press Release, US Office of Public Affairs, 16th October, 2019. Available: https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child (Accessed 11/04/2020)
[26] South Korean Police Agency, Statement, Thursday 17th October, 2020. Available: https://m.police.go.kr/m/bbs/view.do?nttId=22470&bbsId=B0000011&menuNo=2600252&delCode=0 (Accessed 14/04/2020)
[27] United States Department of Justice, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin*, Press Release, US Office of Public Affairs, 16th October, 2019. Available: https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child (Accessed 11/04/2020)
[28] Yongsoo Lee, Deputy Permanent Representative of the Republic of Korea to the United Nations, Plenary Statement at Opening of the 61st Session of the Commission on Narcotic Drugs, Vienna, 12th March, 2018
[29] S2W ab, Mission Statement, Available: http://en.s2wlab.com/Company (Accessed 07/04/2020)
[30] S2WLab, Products: S2-Eyez, Key Features, Available: http://en.s2wlab.com/s2-eyez (Accessed 08/04/2020)
[31] S2WLab, Products: S2-Eyez, Key Features, Available: http://en.s2wlab.com/s2-eyez (Accessed 08/04/2020)
[32] S2WLab, Products: S2-Eyez, Key Features, Available: http://en.s2wlab.com/s2-eyez (Accessed 08/04/2020)
[33] S2WLab, Products: S2-Eyez, Key Features, Available: http://en.s2wlab.com/s2-eyez (Accessed 08/04/2020)
[34] Suh Sanduk quoted in: Samuel Haig, *Interpol Enlists Korean Startup to Track Crypto on the Dark Web*, CoinTelegraph, 21st March, 2020. Available: https://cointelegraph.com/news/interpol-enlists-korean-startup-to-track-crypto-on-the-dark-web (Accessed 15/04/2020)
[35] Naver (News.Naver.com), *Domestic Dark Web Professional Analysis Startup S2W "You need to pre-block virtual currency blacklists"*, 26th March, 2020, (Translated from Korean). Available: https://n.news.naver.com/article/023/0003518262?sid=105 (Accessed 08/04/2020)
[36] Stephen White, *#Privacy: Interpol Receives Support from South Korean Cyber Intelligence*, PrivSec Report, 23rd March, 2020. Available: https://gdpr.report/news/2020/03/23/privacy-interpol-receives-support-from-south-korea-cyber-intelligence/ (Accessed 03/04/2020)
[37] Suh Sanduk quoted in: Samuel Haig, *Interpol Enlists Korean Startup to Track Crypto on the Dark Web*, CoinTelegraph, 21st March, 2020. Available: https://cointelegraph.com/news/interpol-enlists-korean-startup-to-track-crypto-on-the-dark-web (Accessed 15/04/2020)
[38] Naver (News.Naver.com), *Dark Web International Investigation Assistance,* 4th March, 2020, (Translated from Korean). Available:

https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=030&aid=0002870806 (Accessed 12/04/2020)

[39] Alois Afilipoaie & Patrick Shortis, *Cryptomarket Enforcement – New Strategy and Tactics*, Situation Analysis, Global Drug Policy Observatory, June 2018

[40] The CND is the central policymaking body within the United Nations system dealing with drug-related matters

[41] UNODC/HONLAP/43/6, *Report of the Forty-Third Meeting of Heads of National Drug Law Enforcement Agencies, Asia and the Pacific* (Bangkok 22-25 October, 2019), 14th November, 2019, P. 7

[42] UNODC/HONLAP/43/6, *Report of the Forty-Third Meeting of Heads of National Drug Law Enforcement Agencies, Asia and the Pacific* (Bangkok 22-25 October, 2019), 14th November, 2019, P. 7

[43] Yongsoo Lee, Deputy Permanent Representative of the Republic of Korea to the United Nations, Plenary Statement at Opening of the 63rd Session of the Commission on Narcotic Drugs, Vienna, 2nd March, 2020

[44] Yongsoo Lee, Deputy Permanent Representative of the Republic of Korea to the United Nations, Plenary Statement at Opening of the 61st Session of the Commission on Narcotic Drugs, Vienna, 12th March, 2018