Beyond Lies[1]

by

Hermawan Sulistyo[2]
Conflict Historian
Chair, Center for National Security Studies

a paper

The International Studium Generale
on
Cybercrime and Cybersecurity
in Indonesia and Singapore

a joint session

School of Law
and
Center for National Security Studies
Universitas Bhayangkara Jakarta Raya
(Ubhara Jaya)

Bekasi, August 19, 2019

[1] Anditto Heristyo from Digital Garage Tokyo contributed parts of this paper. A mathematician, he is a geek in Algorythm, Block Chain and Cryptology. Yet, none of his opinion expressed here represents Digital Garage.

[2] Conflict historian Professor Hermawan Sulistyo is research professor at the Indonesian Institute of Sciences (LIPI). He is Chair of the Center for National Security Studies at Universitas Bhayangkara Jakarta Raya. He is teaching at the Indonesian Police College (PTIK). He received his PhD from Arizona State University and was once a scholar-in-residence at ISEAS Singapore. He has published numerous books and articles.

I. **Apetizer**

When Kaku wrote in 1997,[3] that developments in computer science—as one of the three pillars of science—contribute to the rapid changes of everything, the enterprose had already been there. In the past couple years IT and telecommunication technology have not only changed the international socio-political and economic landscape but also individual human behavior as well. The technology brings its positive impacts but at the same time it also entails negative aspects. For one thing, internet and telecommunications technology enables criminals searching new avenues of crime, particularly in transnational crimes. This is not to mention massive use of mobile phones—cheaper and easier to access—that change features of mass cultures in the whole world.

Apart from high-speed pace of developments in the nooks and crannies of technicalities in IT, there are layers of lies beyond lies involved in and being manipulated in the ongoing use of IT in legal, social and political realms. Problems emanates from the IT world does not only concern some issues within the IT itself, such as technological lacks and gaps, but also embraces non-techinical dimensions. This last thing is much more troublesome than technical issues. And thus, contents must be read beyond the lines, where falsehood, lies, hoax and fraud occupy the space.

As occured anywhere, computers are not a luxury item any longer. Even more so is mobile phones. They are relatively cheap with much now easy and convenient accesses. And yet, with about half of the 260 million people of Indonesia have only graduated from elementary schools it is only logical that mobile phone users are prone to hoax and other internet fraud. It is more complicated when dealing with political and social issues. As the nation is moving toward democratic society, unavoidably entangled political and social dimensions contribute much to the national political stability. Internet and moblie phone become effective political instruments.

IT may be used to boost national interests under the rubric of national security of every .bilateral and multilateral confrontation-cooperation in IT and telecommunications become critical. As shown in the attached Summary on Current Trends in Internet and Computer Security, it is clear that the more the technology develops, the more loopholes for fraud and crimes are available.

II. Entree: Lesson from Indonesia

In terms of transnational telecommunications and internet fraud, cases involving citizens of PRC and ROC are increasing in staggering number every year (see attached data), despite INP efforts to control the crimes by stern measures. And for various apparent reasons the INP needs technical cooperation from their foreign counterparts. IPP and other computer data for instance. But not only these technicalities.

[3] Michio Kaku, *Visions.* New York; Anchor, 1998.

Language is another problem. Almost none of the INP officers do not speak Chinese (Mandarin or else), while the suspects do not speak Indonesian. Often both parties communicate with below-average English language skills. The problem is more complicated when they use small cities as their operation bases. Language barrier is a problem. A presence of counteropart's police officers is then almost-a-must situation. Even in such a more conducive situation, sometimes distrust still lingers. A foreign counterpart officer who has known much of his/her local-host culture, such as Mr Jay Lee of ROC, would have made legal process much easier.

Modus of the telecommunications and computer/internet crimes is that the perpetrators usually contact the potential preys, claiming they are from law enforcement agencies or other administration offices such as police, AG, tax and customs, bank in their home country. The fake identities used are made according to the types of fraud they would have done. All victims of fraud reside and live in their home country: mainland China or Taiwan. The perpetrators would then ask targeted potential victims to transfer certain amount of money to a designeted bank account in the PRC and ROC.

The perpetrators master skills in IT to erase evidence when caught. With fake IDs they rent houses for US$ 3,000-4,500 per month—considered expensive by local standard—and rent high speed internet access--over 10 Mbps/mo. They never go outside the house; household shopping and other outside activities are done by Indonesian helpers. It is suspected that perpetrators' network operate in some ASEAN countries.

Many cases of transnational telecommunications fraud in Indonesia involving PRC citizens are uncovered through coordination between the INP and CID of the Public Security Ministry of the PRC and ROC's counterparts. The counterparts coming to Indonesia bringing with them data on IP addresses which are still active in Indonesia. The data make it easier for the INP officers to track down perpetrators house. Proofs of evidence usually include passports, IDs, mobile phones, laptop, printer, flash disk, hard disk, modem, wireless router, VoIP gateway, voice recorder, credit card skimmer, documents, calculator, Indonesian IDR money and various other hard currencies.

The perpetrators operate from several cities such as Jakarta, Tangerang (Banten Province), Bogor (West Java), Bandung (Capital of West Java Province), City of Banten (Banten Province), Cirebon (West Java Province), Semarang (Capital of Central Java Province), Surakarta (Central Java), Sleman (Yogyakarta Special Province), Surabaya (Capital of East Java), Denpasar (Bali), Medan (North Sumatera), Batam (Riau Islands), Tanjung Pinang (Riau Islands), Balikpapan (East Kalimantan), Pontianak (West Kalimantan) and Manado (Capital of North Sulawesi). They use those cities as their home base for their operations.

For the ambush and arrests the central INP headquarters coordinated with local police offices. Ambush and arrests are conducted simultaneously to prevent the evidence from missing and the perpetrators run away. After the arrests, INP processed all cases and then sending the perpetrators to the Immigration for further legal actions, such as deportation. The INP provides black listed names and red notice to the immigration offices.

This INP-Immigration processes is very effective and efficient to track down someone's criminal records in telecommunications and IT fraud. Thus it might be possible to share criminal data with counterparts from other countries. When the perpetrators are trying to return to Indonesia, the Indonesian Immigration offices have had their previous criminal data. No-entry decision could be made from the beginning, as early as possible. Now, Indonesia is no longer a haven for telecommunications and IT fraud, as it used to be notoriusly known.

III. A Summary of Current Trends in Internet & Computer Security

It has evolved way beyond individual attacks by Nigerian spam & virus attachment files, and the "lone hacker" archetype, into sophisticated large-scale attacks, including state-sponsored attacks. In the end, every security system is only as strong as it's weakest component. And in most systems, the weakest link is the human factor.

Many things are so integrated that even experts can be conned with a sophisticated social engineering attack. In perspective of the common user, who might not be technologically savvy, much effort has been integrating security into the system seamlessly. Ideally, users does not think twice, and behaves securely as a default behavior.

1. HTTPS is becoming the default settings

HTTPS guarantees that you connect to the intended domain for authentication purposes, and provides data privacy & integrity, preventing man-in-the-middle attacks. It is superior to calregular HTTP in every way, and from the developer or business owner's perspective, is also becoming easier to integrate with the prevalence of LetsEncrypt [1]. As a result, from 2018 more than 50% of the top 1 million websites use HTTPS as a default redirection [2]. Another factor, most major Internet browsers such as Chrome and Firefox clearly indicate HTTPS websites, and warn users when they are accessing a plain HTTP website. This instills the habit of using HTTPS even on non-technical users, and puts social pressure on website administrators to integrate HTTPS onto their site.

[1]https://www.eff.org/deeplinks/2018/02/lets-encrypt-hits-50-million-active-certificates-and-counting

[2]https://www.theregister.co.uk/2018/08/28/web_security_sitrep/

2. Identity theft / accounts

As the number of accounts of various services increase, it becomes much harder to manage your passwords. An attack through brute-forcing weak passwords remains a risk, but with the popularization of password manager systems like 1Password & LastPass, people have shifted to choosing stronger, non-memorable passwords and managing them, as opposed to choosing weak passwords to remember [3]. For many web services, 2-factor authentication systems, where sites require another authentication key besides the password is also becoming the norm. Some even realize that the act of mitigating fraudulent logins reduces claims from users, and thus increases profits. As such, they encourage users to use 2-factor authentication with built-in incentives [4]. On the other hand, the weakest link in security is the human element, and in many cases a 2-factor authentication system might actually be a security flaw. In particular, authentication through SMS is especially vulnerable to SIM or phone related attacks, such as SIM cloning attacks [5].

[3]http://www.cloudpro.co.uk/it-infrastructure/security/7607/how-to-master-your-passwords-on-all-your-devices

[4]https://www.engadget.com/2018/09/05/ubisoft-rewards-2fa-with-rainbow-six-siege-skin/

[5]https://www.digitaltrends.com/mobile/sim-swap-fraud-explained/

3. Malware and the common virus are at a downtrend

Spam filters & virus scanners are more sophisticated, and integrated into most email clients and operating systems. Updates are also more frequent and can be automated, mitigating vulnerabilities through software bugs and zero-day exploits. People also tend to be more aware about not opening unexpected files from unknown addresses. The usage of ad blockers are also more common in web browsers, so attacks through fraudulent ads are less prevalent as well [6]. Even in the cases where a computer becomes infected, common viruses are not as prevalent as before. Instead, hidden cryptocurrency miners, in which the payload secretly mines cryptocurrency secretly using the infected computer's resources is becoming more common [7].

[6]https://marketingland.com/survey-shows-us-ad-blocking-usage-40-percent-laptops-15-percent-mobile-216324

[7]https://www.zdnet.com/article/why-cryptocurrency-mining-malware-is-the-new-ransomware/

4. Large scale public opinion-changing social attacks

On a larger scale, (allegedly) state-sponsored attacks through social media are suspected to have a major effect in controlling the public opinion. One of the biggest evidence currently being scrutinized is Trump's possible collusion with Russia during the US elections [8]. Through use of fake sites, fake news, and sock puppet accounts, this type of attack can aim to sow doubt, spread false facts, start dissenting public opinion, and/or polarize the target audience. Popular social media such as Facebook and Twitter is the new cyber-warfare battlegrounds [9]. In Indonesia, a similar case can be observed through the Saracen incident [10]. With the Presidential Elections coming up in 2019, such attacks are quite possibly already occurring.

[8]https://www.cnbc.com/2018/02/17/facebooks-vp-of-ads-says-russian-meddling-aimed-to-divide-us.html

[9]https://www.vox.com/2018/7/31/17635592/facebook-elections-russia-2018-midterms

[10] https://id.wikipedia.org/wiki/Saracen_(Indonesia)

5. Hacks of large silos of Big Data

With the trend of moving big data onto the "cloud", cluster of data collected in one place is attractive to hackers. As an example, one of the biggest hacking incidents was the Equifax hack, where sensitive data of over 500 millions of Americans were breached [11]. Internet giant Yahoo was also attacked, with a data breach of all 3 billion accounts they possess [12].

[11]https://money.cnn.com/2018/02/09/pf/equifax-hack-senate-disclosure/index.html

[12] https://www.wired.com/story/worst-hacks-2017/

6. Rise of cryptocurrencies

Through cryptocurrencies, moving money across borders becomes much easier. Besides using blockchain analysis, the exchanges where people can trade their cryptocurrency with fiat money tend to be regulated, with customer identification required for KYC (Know Your Customer) or AML (Anti-Money Laundering). There are decentralized exchanges where customers are not tracked, but governments are starting to put pressure for them to comply [13].

IV. Attachment

Police to Combat Transnational Telecommunicatiom Fraud

Cybercrime is something new to the police; hardware and software resources are still, and always lacking to the need of contestation between the good use and the bad use of IT. Particularly difficult is when dealing with contents which contain hoax, lies and hate speech. Hate speech in slandering someone may result in personal feud. But when it comes to public sphere the result of the "crime" might be devastating.

Data shows that cybercrime is becoming more and more problematic for the Indonesia in terms of it's national unity. Cybercrime creates socio-political divisions among the less educated society.

No	Case	Year						KET
		2013	2014	2015	2016	2017	2018	
1.	Email fraud	26	868	3216	[redacted]			
2.	Web fraud	538						
3.	Credit card fraud	17						
4.	Comm. ftaud	540						
5.	Defacing/Hacking	34	44	54	42	68	13	
6.	Online porn	48	56	284	155	181	117	

7.	Child porn							
8.	Online gambling	9	15	38	26	21	23	
9.	Identity theft	16	16	100	20	33	30	
10.	Defamation	118	254	1248	845	853	608	
11.	Extortion			36	17	28	14	
12.	Hate speech			76	91	105	35	
13.	Threat			184	108	115	74	
14.	Illegal access			216	147	141	131	
15.	Illegal intercept			14	15	20	1	
16.	DDoS			82	71	20		
17.	TPPU			30				
18.	Stealing				2			
19.	Cheating				4506	1312	701	
20.	Relogious/racial						131	
21.	Other cases	59	53					
	Total	**1405**	**1306**	**5578**	**6045**	**2897**	**1878**	

Collected data available since 2013, all foreihgn nationals **(PRC and RoC)** detained is as follows:

1. 28/11/2013: 48 persons in BSD Tangerang (Subdit Cyber Bareskrim Polri)
2. 15/07/2014: 90 persons in Jakarta (Subdit Cyber Bareskrim Polri)
3. 21/07/2014: 56 orang di Semarang dan Batam (Subdit Cyber Bareskrim Polri)
4. 22/08/2014: 9 persons in Surakarta (based on information from the public)
5. 18/10/2014: 22 persons in Pontianak Kalbar (based on information from the public)
6. 30/10/2014: 57 persons in Balikpapan, East Kalimantan (based on information from the public)
7. 18/10/2014: 65 orang di Jakarta (Subdit Cyber Bareskrim Polri)
8. 04/04/2015: 39 persons in Bali (Subdit Cyber Bareskrim Polri)
9. 28/04/2015: 40 persons in Semarang (Polrestabes Semarang)
10. 06/05/2015: 33 persons in Jakarta Selatan (Subdit Jatanras Pmj)
11. 12/05/2015: 30 persons in Jakarta Utara (Subdit Jatanras Pmj)
12. 24/05/2015: 29 persons in Jakarta (Direktorat Krimum Pmj)

13. 25/06/2015: 53 persons in Batam (Ditkrim Um Polda Kepri).

14. 26/08/2015: 33 persons in Bandung (Dittipidnarkoba & Subdit It & Cc).

15. 27/09/2015: 62 persons in Manado (Dit Reskrimum Polda Sul-Ut)

16. 20/10/2015: 41 persons in Cirebon (Subdit It & Cybercrime Bareskrim)

17. 20/10/2015: 32 persons in Surabaya (Subdit It & Cybercrime Bareskrim)

18. 20/10/2015: 46 persons in Bali (Subdit It & Cybercrime Dittipideksus Bareskrim)

19. 26/11/2015: 25 persons in Jakarta Utara (Jatanras Dit Krimum Pmj)

20. 04/12/2015: 15 persons in Sleman, Yogyakarta (Polres Sleman)

21. 01/02/2016: 8 persons in Jakarta (Ditreskrimsus Polda Metro Jaya)

22. 20/06/2016: 31 persons in Bogor (Polres Bogor)

23. 21/01/2017: 7 persons in Jakarta Utara (atas laporan masyarakat)

24. 29/07/2017: 29 persons in Jakarta (Dittipidsiber dan Ditreskrimsus PMJ)

25. 29/07/2017: 31 persons in Bali (Dittipidsiber dan Ditreskrimsus Bali)

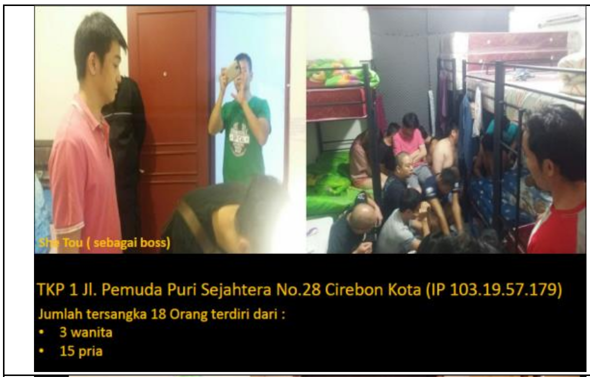
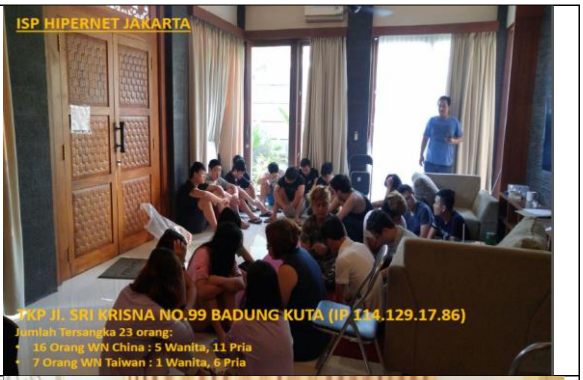
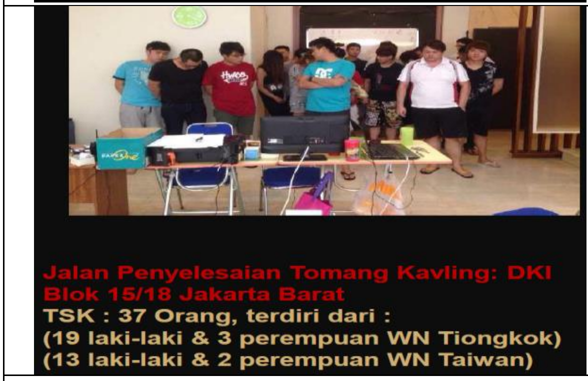
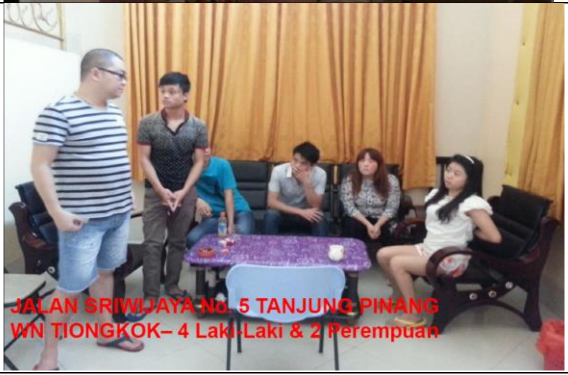
26. 29/07/2017: 93 persons in Surabaya (Dittipidsiber dan Ditreskrimsus Jatim)

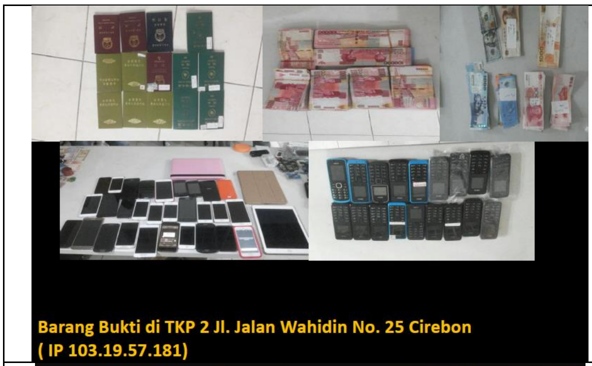
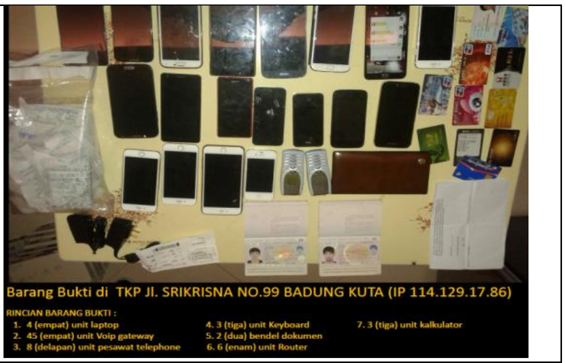
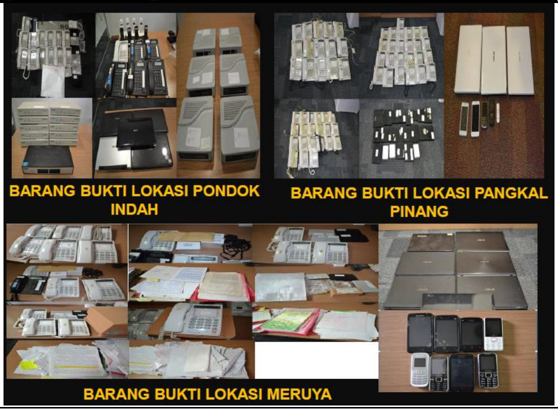
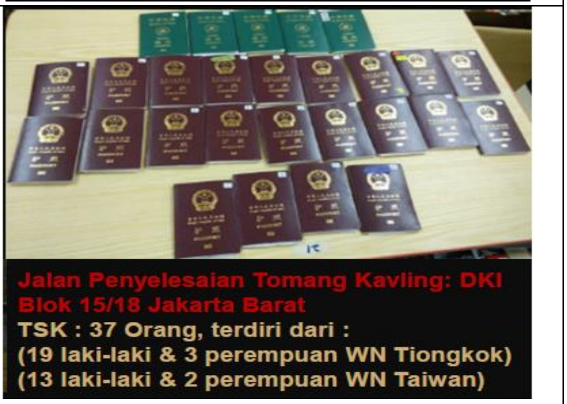
27. 11/01/2018: 64 persons in Bali (Ditreskrimsus Polda Bali)

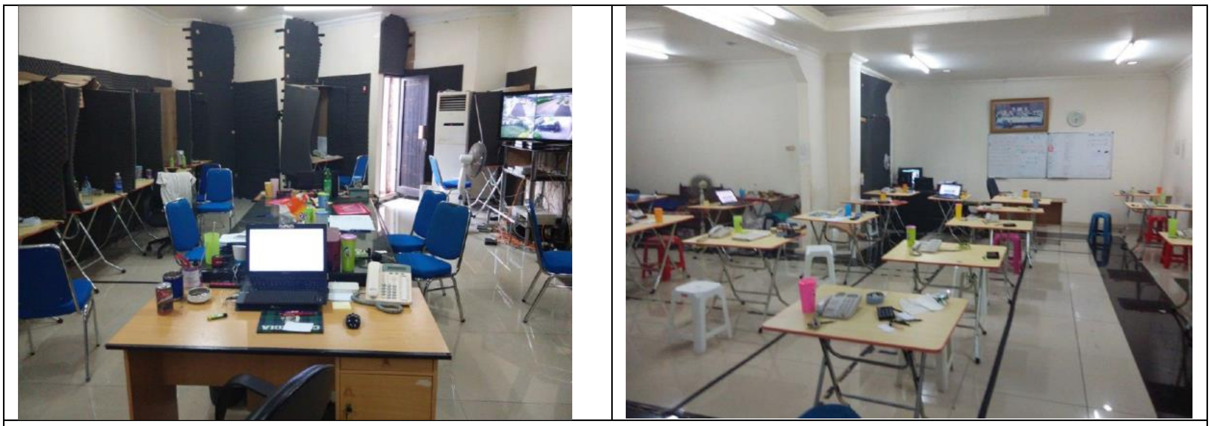
28. 01/05/2018: 103 persons in Bali, (Ditreskrimsus Polda Bali)

ISP CIREBON
TKP 1: JI. PEMUDA PURI SEJAHTERA NO.28 CIREBON KOTA
(IP 103.19.57.179)
ISP BANTEN
TKP 2 : JI. AGUNG PERKASA BLOK J 15, SUNTER, JAKARTA UTARA
(IP 103.244.207.202 , 103.244.207.50 , 103.244.207.118)
ISP BALI
TKP : PERUMAHAN GRAHA SINGKEP ASRI (IP 202.164.217.122)
(Rumah Kosong)
ISP BATAM
TKP : PERUMAHAN VILLA PANBIL BLOK N 26
(IP 103.246.0.41 sudah tidak aktif lagi)

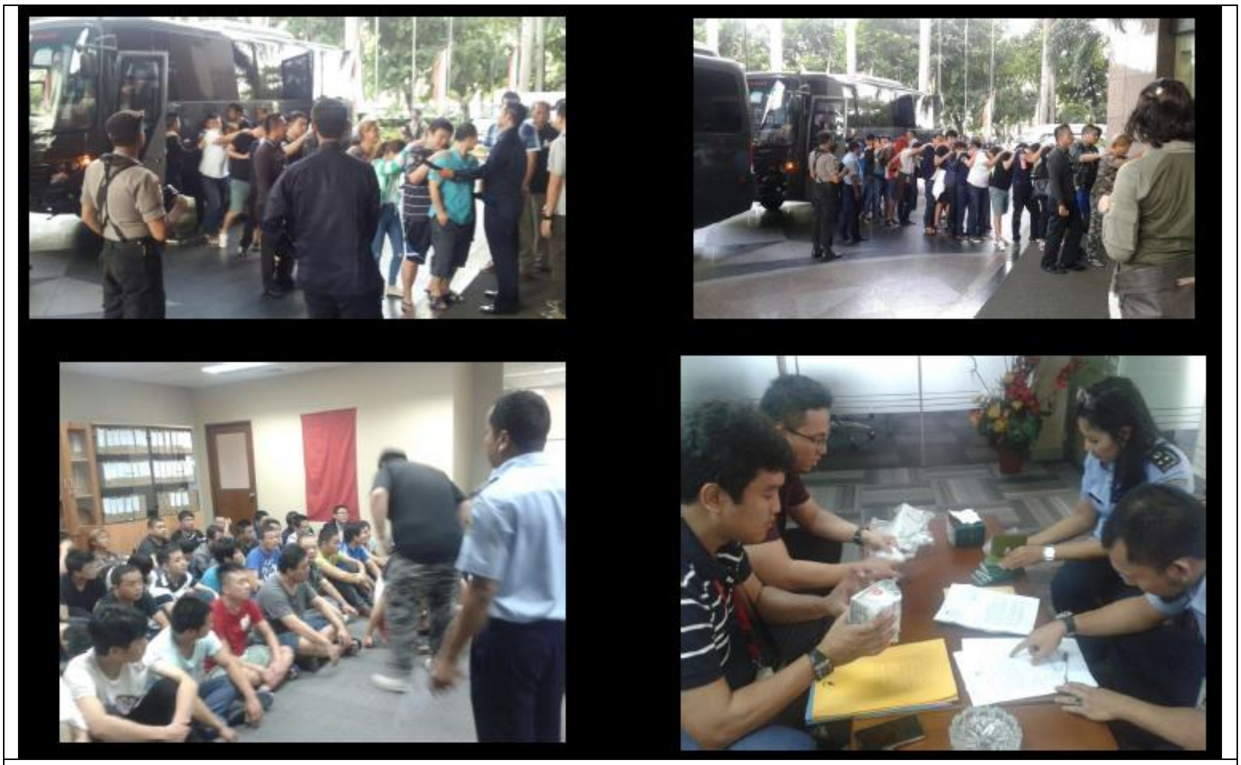
Rented house

 She Tou (sebagai boss) TKP 1 Jl. Pemuda Puri Sejahtera No.28 Cirebon Kota (IP 103.19.57.179) Jumlah tersangka 18 Orang terdiri dari : • 3 wanita • 15 pria	 ISP HIPERNET JAKARTA TKP Jl. SRI KRISNA NO.99 BADUNG KUTA (IP 114.129.17.86) Jumlah Tersangka 23 orang: • 16 Orang WN China : 5 Wanita, 11 Pria • 7 Orang WN Taiwan : 1 Wanita, 6 Pria
 Jalan Penyelesaian Tomang Kavling: DKI Blok 15/18 Jakarta Barat TSK : 37 Orang, terdiri dari : (19 laki-laki & 3 perempuan WN Tiongkok) (13 laki-laki & 2 perempuan WN Taiwan)	 JALAN SRIWIJAYA No. 5 TANJUNG PINANG WN TIONGKOK– 4 Laki-Laki & 2 Perempuan
Perpetrators	

 Barang Bukti di TKP 2 Jl. Jalan Wahidin No. 25 Cirebon (IP 103.19.57.181)	 Barang Bukti di TKP Jl. SRIKRISNA NO.99 BADUNG KUTA (IP 114.129.17.86) RINCIAN BARANG BUKTI : 1. 4 (empat) unit laptop 2. 45 (empat) unit Voip gateway 3. 8 (delapan) unit pesawat telephone 4. 3 (tiga) unit Keyboard 5. 2 (dua) bendel dokumen 6. 6 (enam) unit Router 7. 3 (tiga) unit kalkulator
 BARANG BUKTI LOKASI PONDOK INDAH BARANG BUKTI LOKASI PANGKAL PINANG BARANG BUKTI LOKASI MERUYA	 Jalan Penyelesaian Tomang Kavling: DKI Blok 15/18 Jakarta Barat TSK : 37 Orang, terdiri dari : (19 laki-laki & 3 perempuan WN Tiongkok) (13 laki-laki & 2 perempuan WN Taiwan)
Samples of hard evidence	



Perpetrators’ working room



Suspects tranfered from the police to the Immigration office

Dittipidsiber dalam penanganan kejahatan Transnational Fraud yang melibatkan WN China dan Taiwan lebih banyak dilibatkan dalam **bantuan teknis terkait pemeriksaan barang bukti digital**, sedangkan penanganan upaya paksa lebih banyak dilakukan oleh penyidik yang membidangi atau pun kewilayahan.