UNODC
United Nations Office on Drugs and Crime

Regional Office for Southeast Asia and the Pacific

Southeast Asia, emerging crime challenges and the relationship to technology and cybercrime

TIJ Conference Bangkok, January 2019

Presentation structure

- Southeast Asian integration and variable capacities
- Emerging crime challenges
- Recommendations

Connectivity and integration in the ASEAN region

Safeguards must be incorporated in the regional development agenda

- Regional commitments to expand the economic market through integration
- Physical and non-physical barriers are being removed to ensure more practical and efficient border crossings for people, goods, services, and money, accompanied by a number of supporting infrastructure initiatives

Varying capacities and resources

Illicit trade environment index

Source: The Economist Intelligence Unit

Check point in Jiangjong, China

Check point in Tachileik, Myanmar

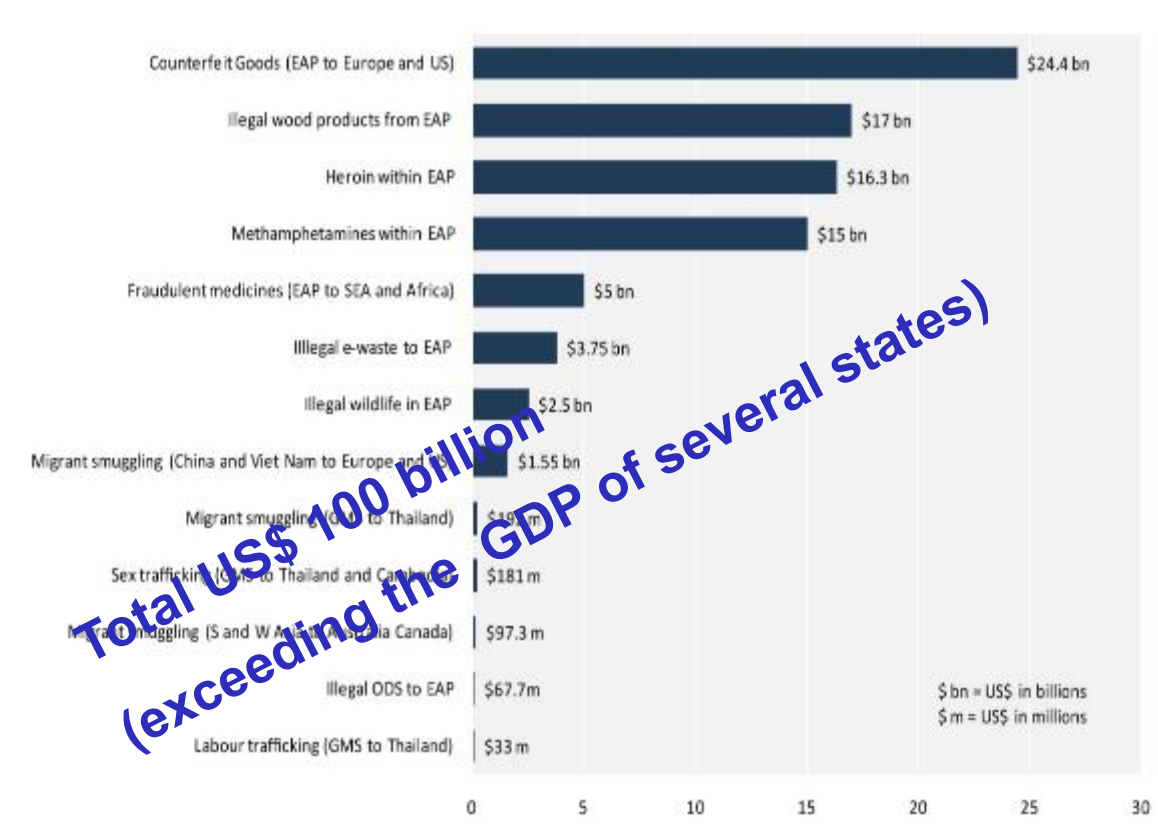
Presentation structure

- Southeast Asian integration and variable capacities
- Emerging crime challenges
- Recommendations

Dark-side of regionalisation: transnational crime contributes to conflict and exposes vulnerabilities

Source: UNODC

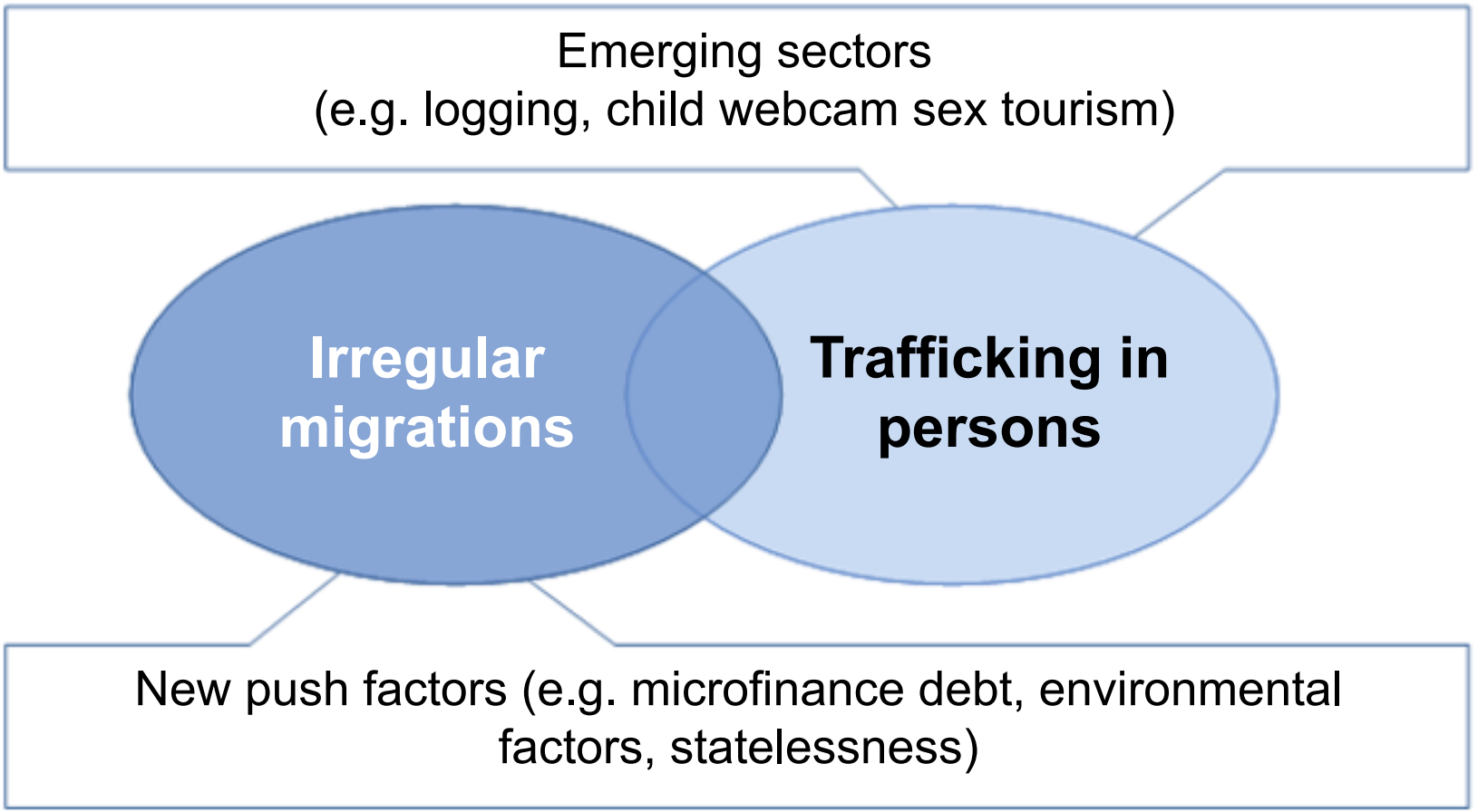
Transnational crime in the region: conservative estimates



Source: UNODC

- Illicit drugs (meth and heroin) : US $40 billion
- Counterfeits : US $30 billion
- Environmental crime : US $24 billion
- People: US $2 billion

Emerging trends in trafficking in persons / smuggling of migrants



Trafficking in persons and smuggling of migrants

Primary maritime smuggling routes within the region

- Songkhla province, Thailand
- 62 undocumented migrants from Myanmar detected
- Destined for Malaysia

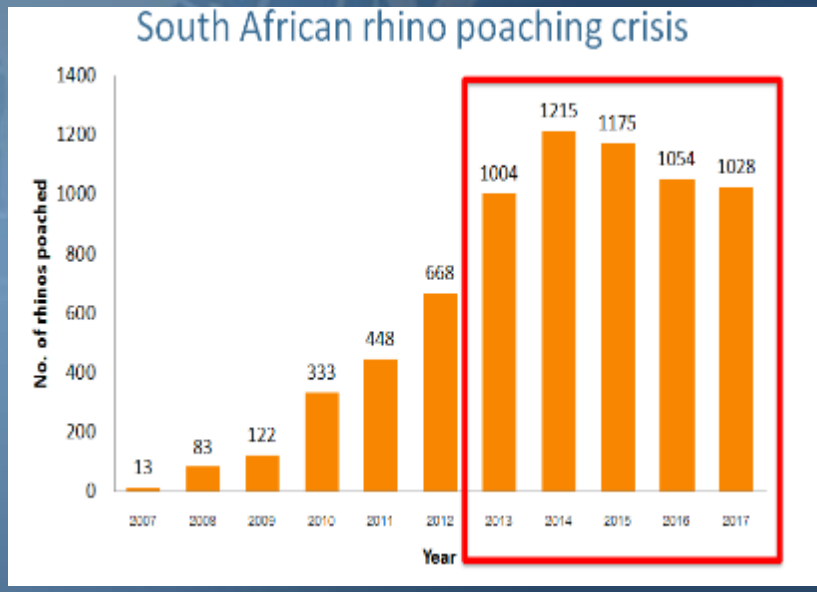
Environmental crimes: wildlife trafficking

Growing in sophistication, scale and profitability

Pangolin

Elephant Ivory

Rhino horn



Source: South Africa Department of Environmental Affairs

- Rapidly growing demand in the region, serving as a major destination
- Extinction of species
- Sophisticated criminal networks operating intra-regionally and inter-regionally
- Inadequate criminal justice responses

Environmental crimes: wildlife trafficking

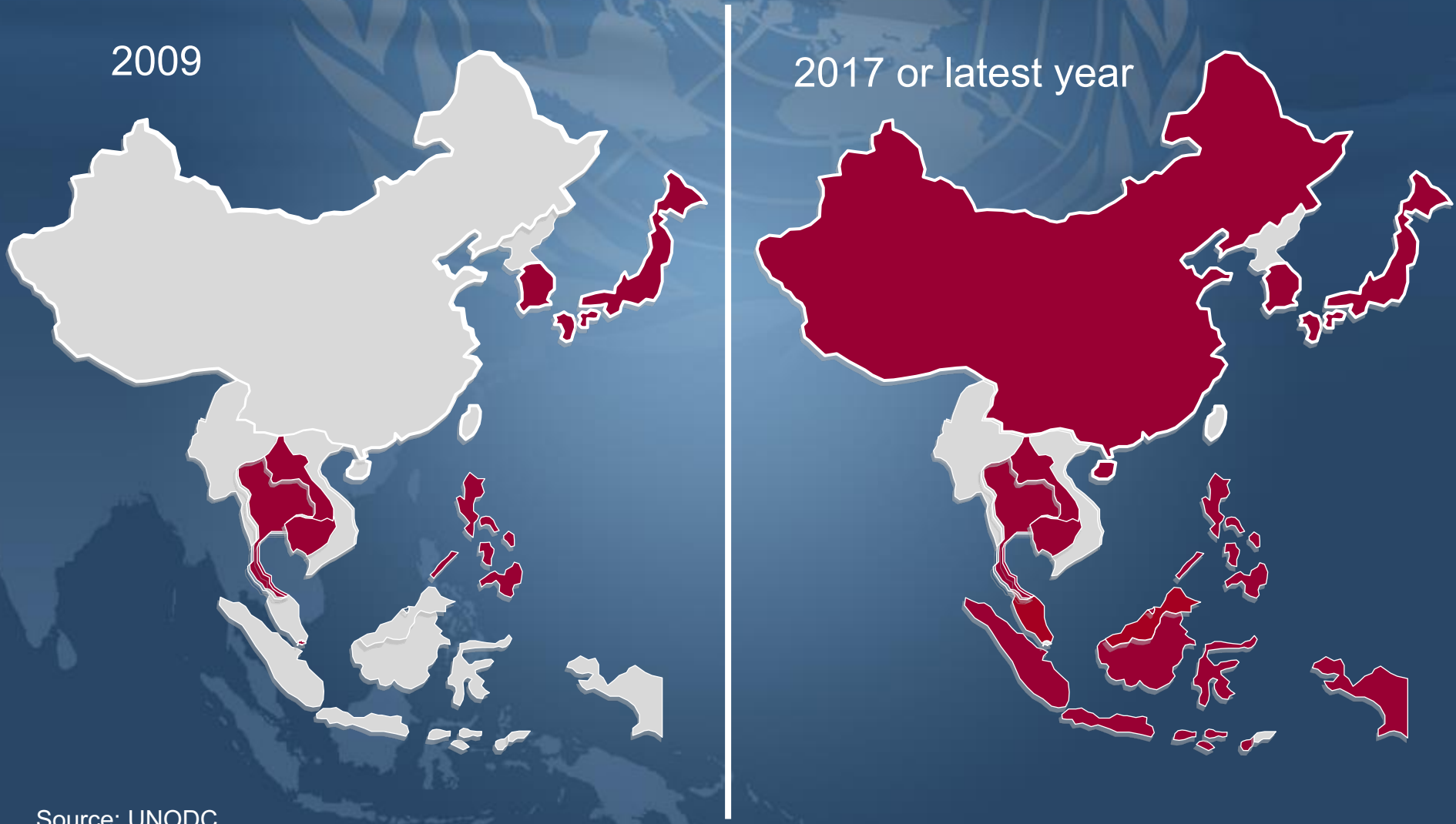
Within the region and increasingly with other regions

- March 2018, Pasir Panjang Scanning Station, Singapore
- 3.5 tons of ivory
- Nigeria – Singapore – Viet Nam

UNODC
United Nations Office on Drugs and Crime

Regional Office for Southeast Asia and the Pacific

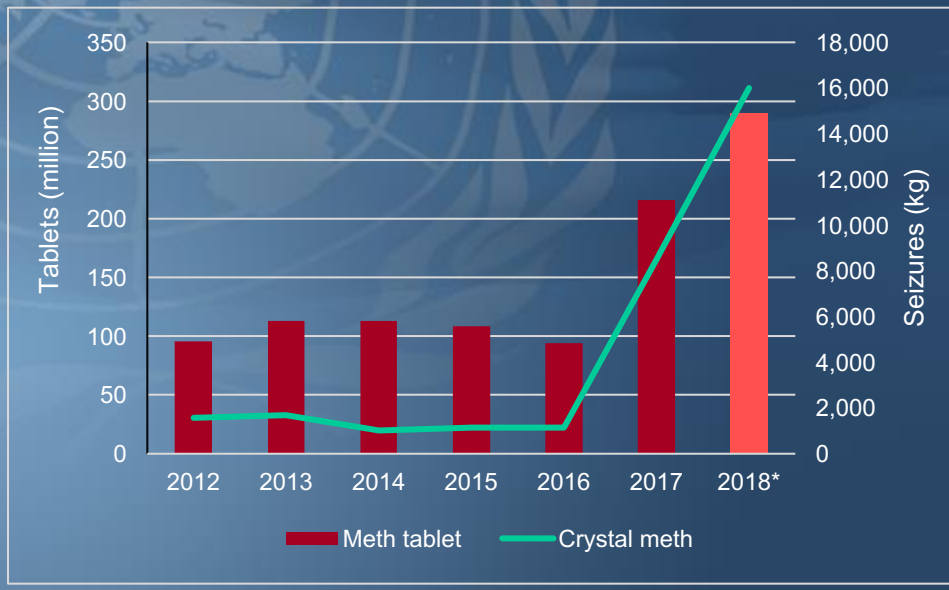
Increasing meth demand in the region



Source: UNODC

Mobility of transnational organized crime groups

Production of synthetic drugs, in particular meth, concentrated to the Golden Triangle



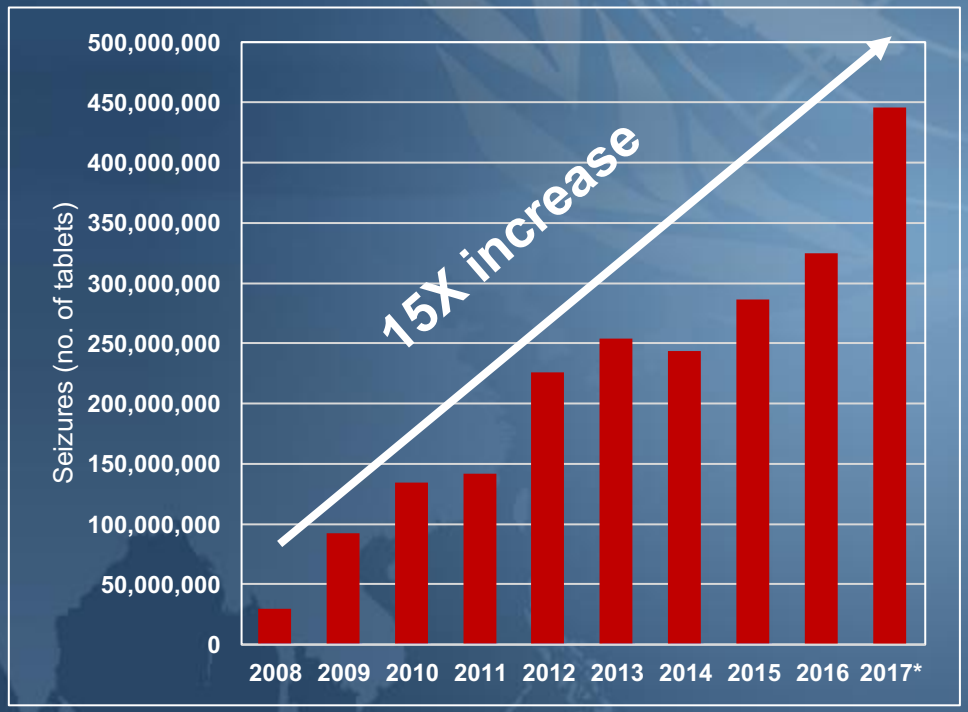
Source: ONCB, Thailand

Seizures of methamphetamine (both tablet and crystalline) in Thailand, 2013 – 2018*

* 2018 data estimated based on seizures reported until 15th August

Meth tablet market in the region

Increasing seizures while price drop across Asia, signalling surge in supply of the drug



Seizures of methamphetamine tablet, 2008 – 2017

	2014	2017
Cambodia	4 – 5	3
Malaysia	10	3.7
Myanmar	3 – 6	1 - 2
Singapore	16 – 20	5.7
Thailand	4 – 7	1.5 – 4.5

Retail prices of meth tablet in USD per tablet

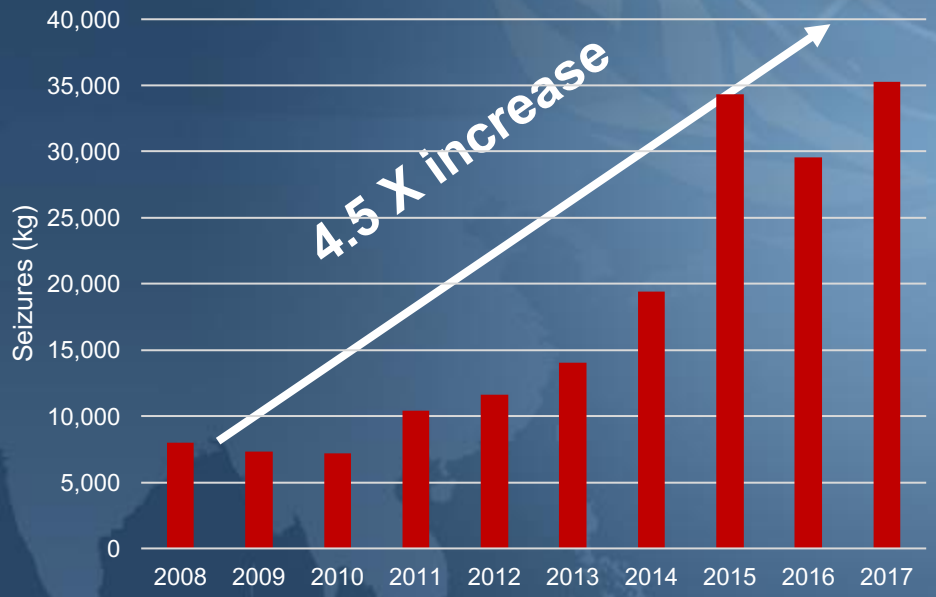
Source: UNODC

Major meth tablet trafficking flows within the Mekong

- 13 – 14 Oct, 2018, Chiang Rai, Thailand, 22 mil meth tablets
- 30th October, 14.6 mil meth tablets seized, the Mekong River, Thailand

Crystal meth market in the region

Increasing seizures while price drop across Asia, signalling surge in supply of the drug



Seizures of crystalline methamphetamine, 2008 – 2017

	2016	2017
China	59	45.6
Indonesia	185 – 190	153 - 185
ROK	422.5	364
Singapore	100 – 120	80 - 100

Retail prices of crystal meth in USD per gram

Source: UNODC

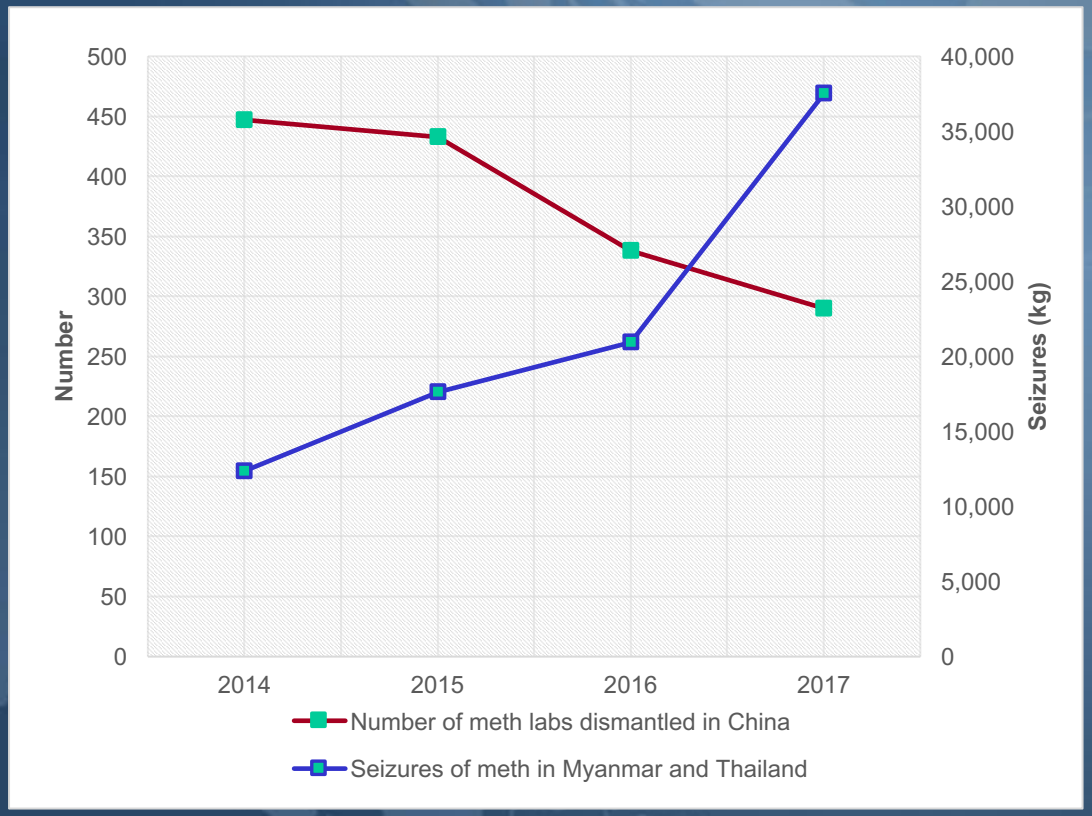
Major maritime crystal meth trafficking flows from the Mekong

- Feb 2018, off the coast of Riau Island
- 1.6 tons of crystal meth
- Destined for Australia and the Philippines

Source: BNN, Indonesia

Analysis on the current meth manufacture situation

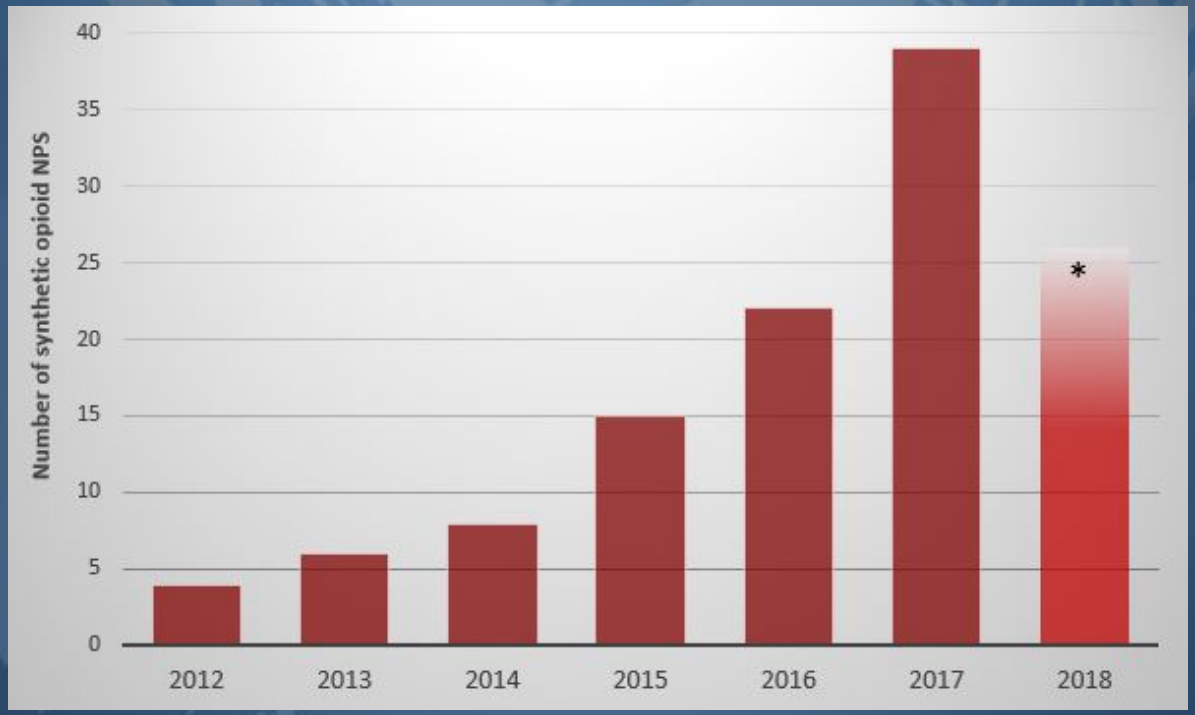
Similar to what we observed in North America more than a decade ago



- Conducive environment in the Golden Triangle pose further challenges:
  - Weak border control
  - Strong ethnic armed groups
  - Surrounded by countries with large and growing chemical / pharma industries

Surge of fentanyl and its analogues

Clandestine manufacturing of fentanyl has risen to connect to existing demand



Number of different NPS with opioid effect reported to the UNODC Early Warning Advisory per year, 2012-2018

Source: UNODC SMART Programme

Growing challenges posed by synthetic opioids

Existing synthetic drug trafficking networks will be increasingly utilised

Source: NNCC, China

- Dec, 2016, Wuhan, China
- Clandestine lab seized with fentanyl, carfentail, furanylfentanyl and other substances

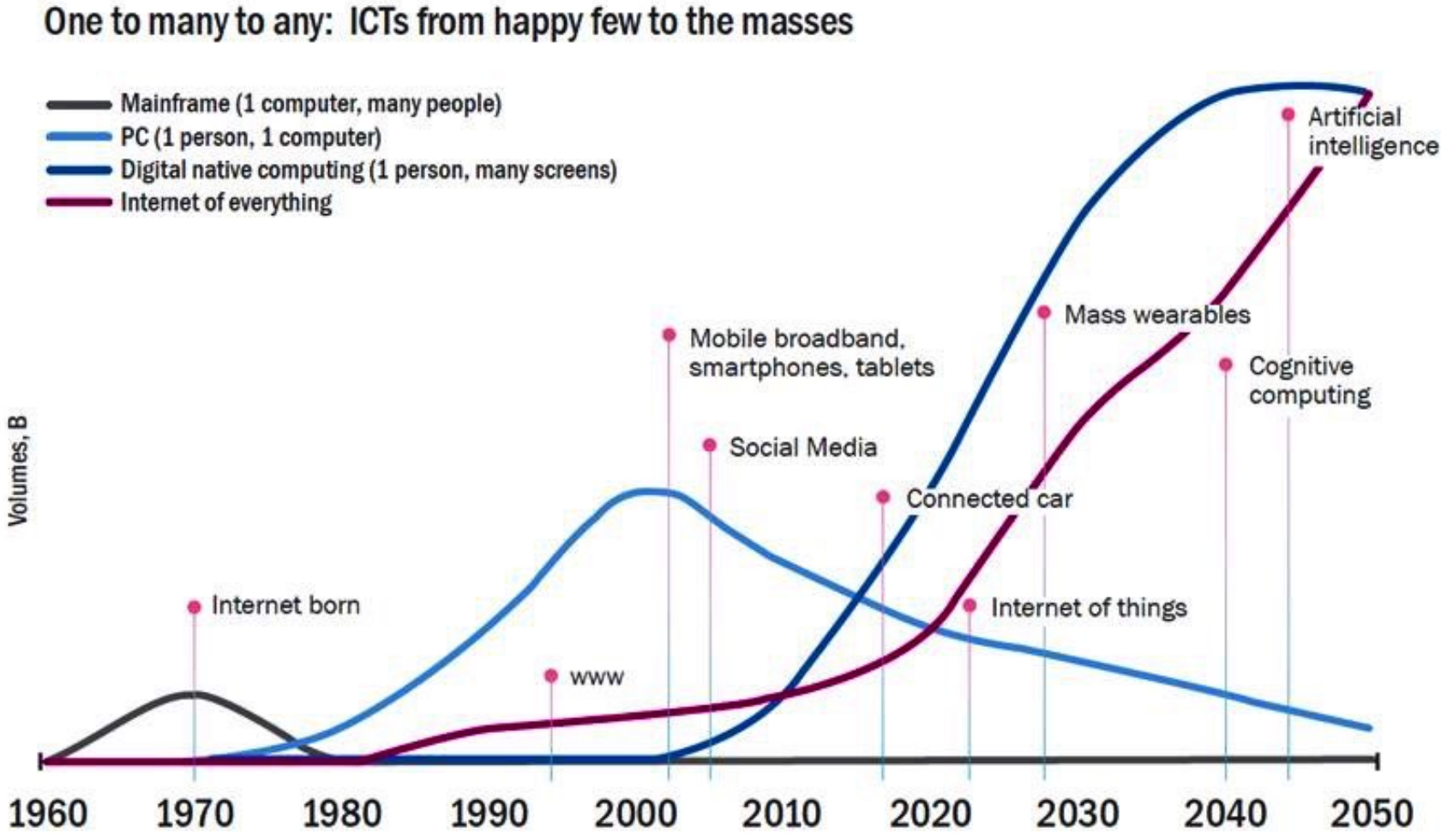
Source: CBSA, Canada

- Jan, 2018, fentanyl departing from Thailand seized in Canada
- First seizure departing from Thailand

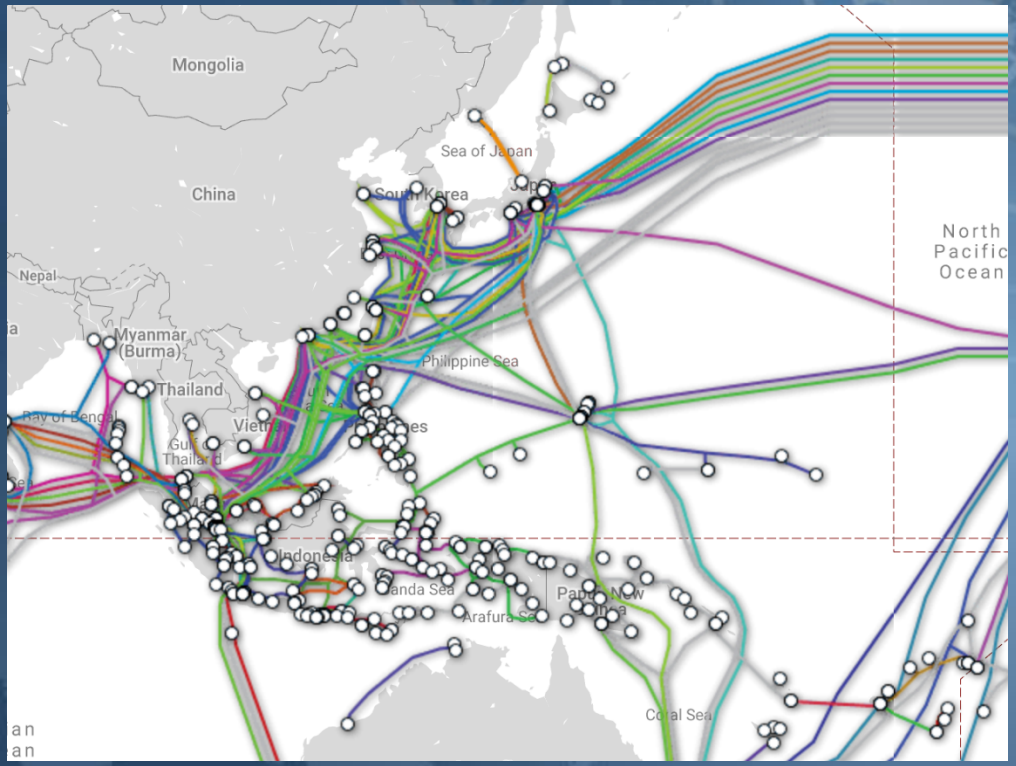
Source: CNB, Singapore

Pills containing fentanyl (Singapore)

HISTORY OF THE FUTURE

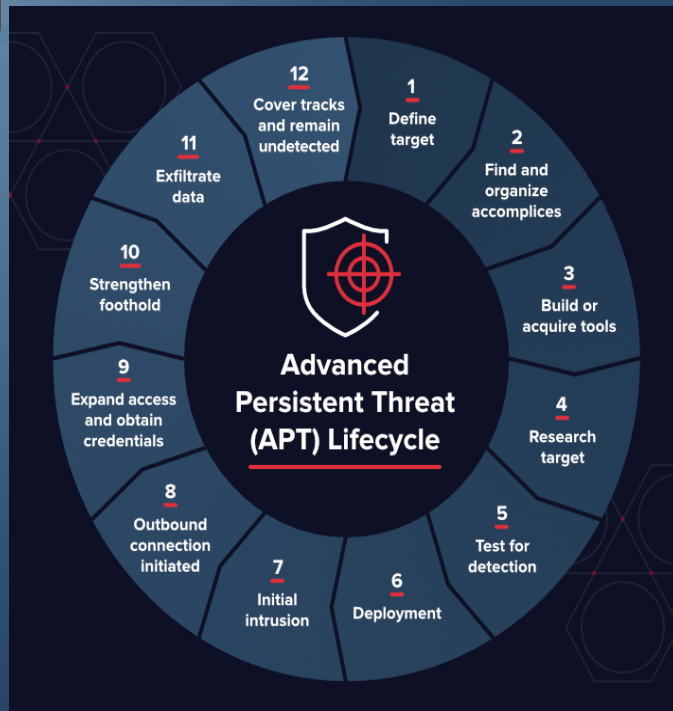


CROSS CONNECTIVITY



BORDERLESS NATURE

- New opportunities for cybercriminals to exploit;
- Destabilizing threat, capitalize and disrupt services associated with critical infrastructure of a nation;
- Needs to be addressed with diplomacy.



UNODC
United Nations Office on Drugs and Crime

Regional Office for Southeast Asia and the Pacific

CYBER RISK IN ASIA

THE SEVERITY OF CYBERATTACKS

in business revenues lost to cyberattacks[1]

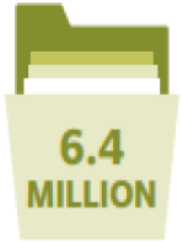
Ranked 5th among Asian top risks[2]

Ranked 6th among Global top risks[2]

RECENT CYBERATTACKS EXAMPLES IN ASIA

personnel stolen from Singapore's defense ministry online database portal in Feb 2017[4]

stolen from cyberattack on a bank in Bangladesh in May 2016[5]



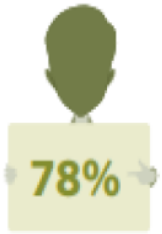
Children's data stolen in Hong Kong hacking of a digital toymaker firm in in Dec 2015[7]

Philippine government websites **simultaneously hacked** in July 2016[6]

ASIAN FIRMS LAG IN CYBERSECURITY

Asian organisations take **1.7 times** longer than the global median to **discover a breach**[8]

Asian firms spent **47%** less on information security than North American firms[9]



of Internet users in Asia have **not received any education** on cybersecurity[10]

CHALLENGES FOR FIRMS IN MANAGING CYBERSECURITY

70% of firms do not have a strong understanding of their cyber posture

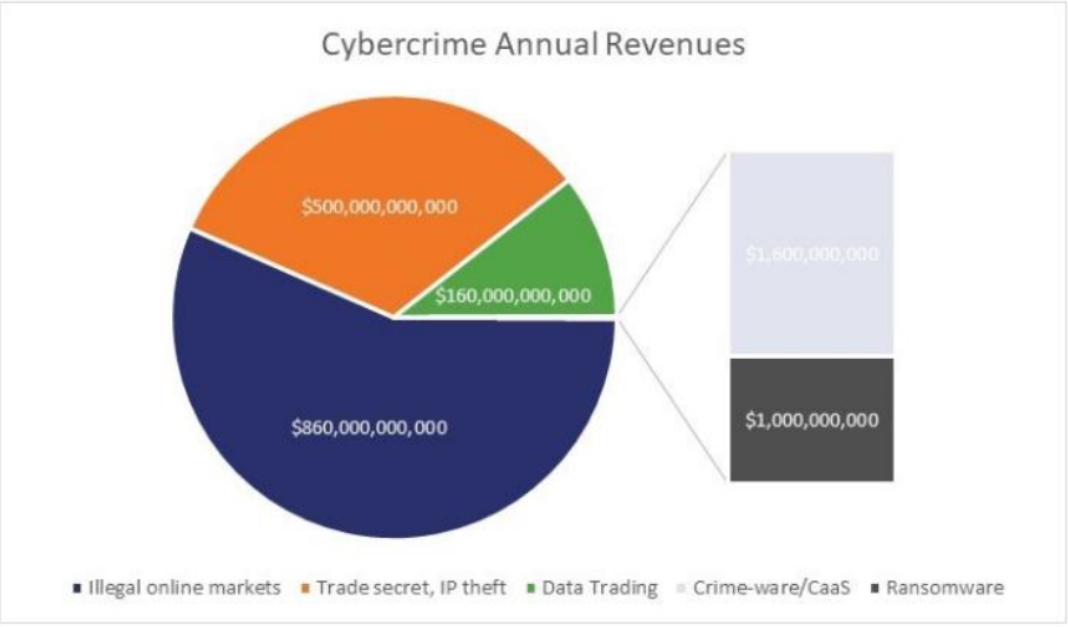
of organisations found it "difficult-to-extremely-difficult" to recruit cyber talent[11]

Primary insurers are reluctant to provide single coverage above **$100 MILLION**

Courtesy of:

MARSH & McLENNAN COMPANIES

CYBERCRIME created over $1.5 trillion USD profits globally in 2018



Crime	Annual Revenues
Illegal online markets	$860 Billion
Trade secret, IP theft	$500 Billion
Data Trading	$160 Billion
Crime-ware/CaaS	$1.6 Billion
Ransomware	$1 Billion
Total Cybercrime Revenues	$1.5 Trillion

Over 50% of cybercrime revenues are generated in online markets

Individual earning potential (in USD)

WHAT CYBERCRIMINALS EARN

- ✓ **Individual hackers** may earn around **$30,000** for one or several jobs; but **platform managers** offering multiple card data forums can **earn up to $2 million.**

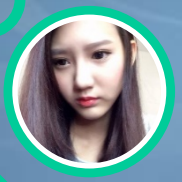
- ✓ **Individual earnings** from **cybercrime** are on **average 10-15% higher** than most traditional crimes.
- ✓ **Earning levels:**
  High earners: $166K+
  Middle earners: $75K+
  Low earners: $3.5K

$ $

CRITICAL ISSUES IN THE REGION

- Fraud
- Business Email Compromise

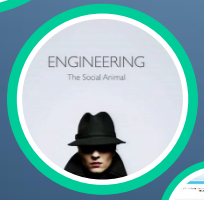
- Software piracy



- Sextortion, Romance SCAMS

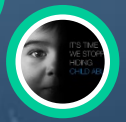
- Malware

- Attacks Against Critical Infrastructure
- Unmonitored and Unpatched IoT devices



- Social Engineering

- Cryptoware

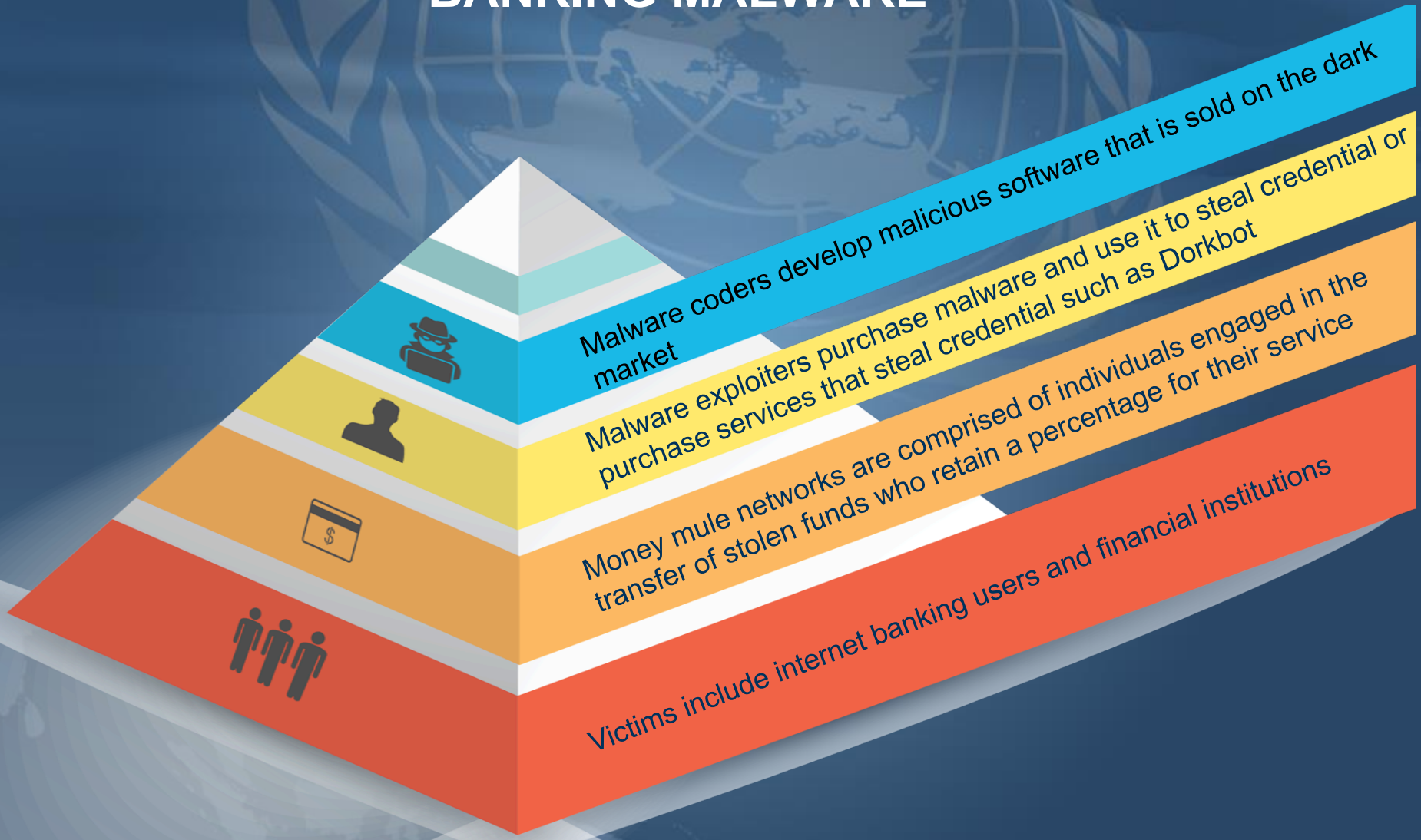


- Online Child Sexual Exploitation

UNODC
United Nations Office on Drugs and Crime

Regional Office for Southeast Asia and the Pacific

BANKING MALWARE



CRYPTOWARE

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/P9VVR3
   http://petya5koahtsf7sv.onion/P9VVR3

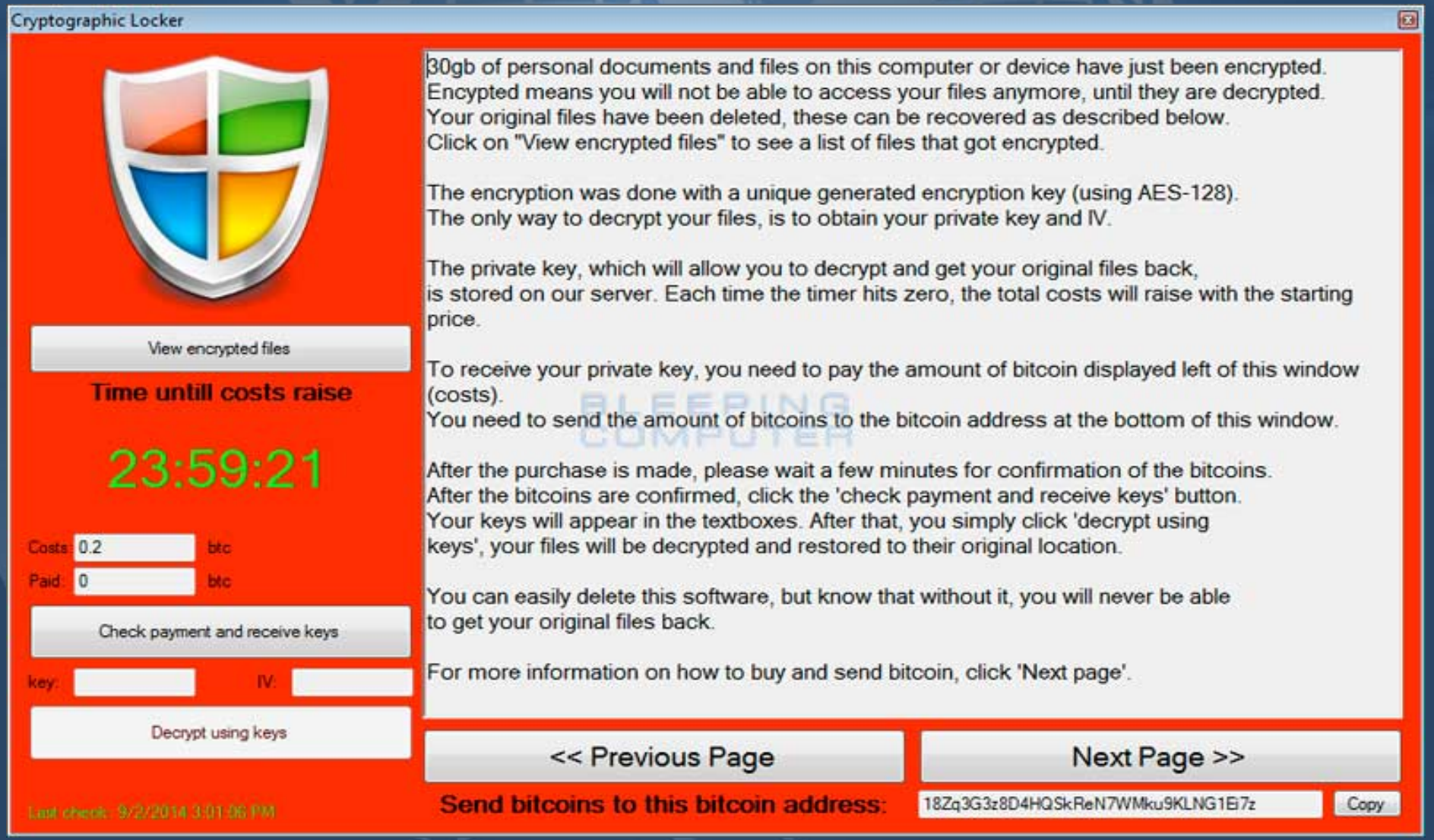
3. Enter your personal decryption code there:

   cdSPP4-JUZrRr-pMSxia-gXpmfB-vGWoRf-FfMph1-XTUzVn-QmFeeV-ofb94y-HuScaa-rB1gmV-djYAEH-8WEakz-wrQ85W-BbsCzw

If you already purchased your key, please enter it below.

Key: 8x3qrMHjmkrN9jfd
Decrypting sector 83234 of 126464 (65%)

RANSOMWARE


Cryptographic Locker
View encrypted files
Time untill costs raise
23:59:21
Costs: 0.2 btc
Paid: 0 btc
Check payment and receive keys
key:
IV:
Decrypt using keys
Last check: 9/2/2014 3:01:06 PM
30gb of personal documents and files on this computer or device have just been encrypted.
Encypted means you will not be able to access your files anymore, until they are decrypted.
Your original files have been deleted, these can be recovered as described below.
Click on "View encrypted files" to see a list of files that got encrypted.
The encryption was done with a unique generated encryption key (using AES-128).
The only way to decrypt your files, is to obtain your private key and IV.
The private key, which will allow you to decrypt and get your original files back,
is stored on our server. Each time the timer hits zero, the total costs will raise with the starting price.
To receive your private key, you need to pay the amount of bitcoin displayed left of this window (costs).
You need to send the amount of bitcoins to the bitcoin address at the bottom of this window.
After the purchase is made, please wait a few minutes for confirmation of the bitcoins.
After the bitcoins are confirmed, click the 'check payment and receive keys' button.
Your keys will appear in the textboxes. After that, you simply click 'decrypt using keys', your files will be decrypted and restored to their original location.
You can easily delete this software, but know that without it, you will never be able to get your original files back.
For more information on how to buy and send bitcoin, click 'Next page'.
<< Previous Page
Next Page >>
Send bitcoins to this bitcoin address:
18Zq3G3z8D4HQSkReN7WMku9KLNG1Ei7z
Copy

How much money does Ransomware make? (in USD)

Ransomware	Date	Profits
CryptoLocker	2013	~$3 million
CryptoWall	2014-2016	~$18-320 million
Locky		$7.8-$150 million
Cerber		$6.9 million
WannaCry	2016	$55,000-$140,000
Petya/NotPetya		$10,000

BUSINESS EMAIL COMPROMISE

Compromising email via social engineering, phishing
Using Non-sophisticated malware e.g. Keylogger

Monitor of email exchange or account takeover
Understanding the business model, activities, relations and etc

Send email to request fund transfer
Via compromised email account or spoof email

Payment transferred
To Criminal's designated account

Money transferred thru network of money mules

A network of criminals orchestrating the scheme

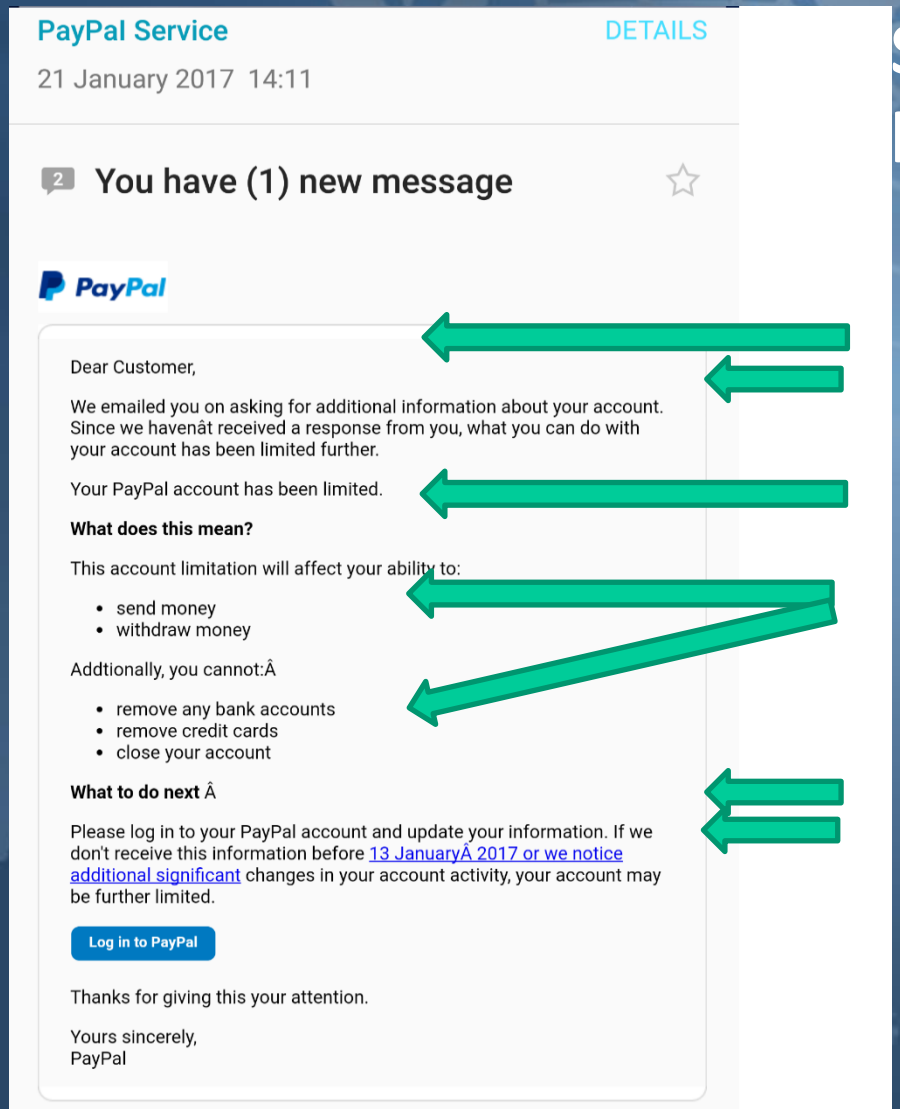
ATM / POS SKIMMING

PRICE: SKIMMER + PIN PAD (OR CAMERA PANEL) $1100 USD WITH SHIPPING INCLUDED

* If you also need MSR reader/writer + 100 blank cards it cost extra 215 USD

DDoS (Distributed Denial of Service)

Phishing & Spear Phishing



PayPal Service DETAILS

21 January 2017 14:11

You have (1) new message

PayPal

Dear Customer,

We emailed you on asking for additional information about your account. Since we havenât received a response from you, what you can do with your account has been limited further.

Your PayPal account has been limited.

What does this mean?

This account limitation will affect your ability to:

- send money
- withdraw money

Addtionally, you cannot:Â

- remove any bank accounts
- remove credit cards
- close your account

What to do next Â

Please log in to your PayPal account and update your information. If we don't receive this information before 13 JanuaryÂ 2017 or we notice additional significant changes in your account activity, your account may be further limited.

Log in to PayPal

Thanks for giving this your attention.

Yours sincerely,
PayPal

Seeing is not necessarily believing!

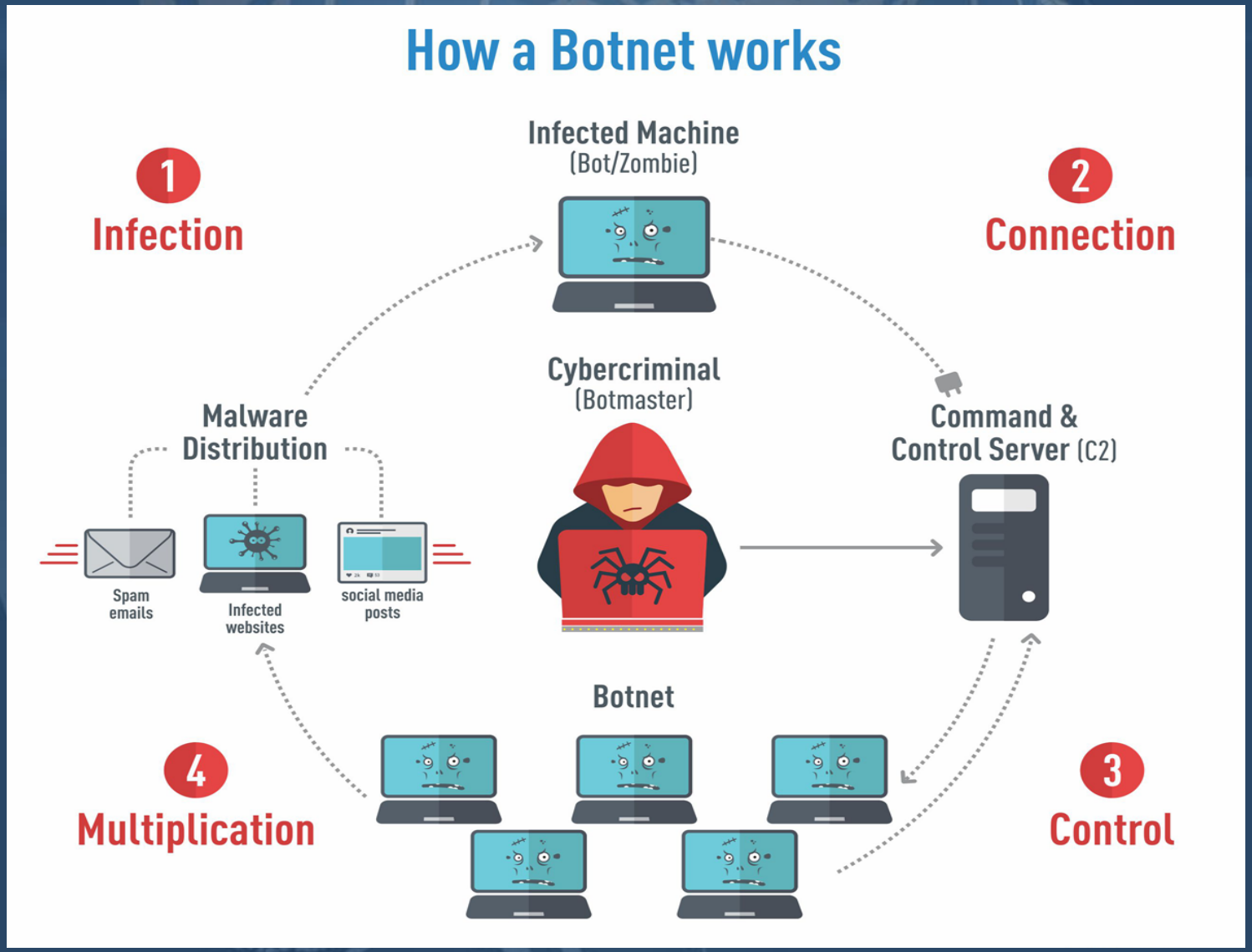
Looks very authentic, doesn't it?

1. Generic Greeting
2. Mistake – date missed out
3. Urgency/threat – Classic sign!

4. Symbols?

5. Incorrect date
6. Poor grammar

BOTNETS

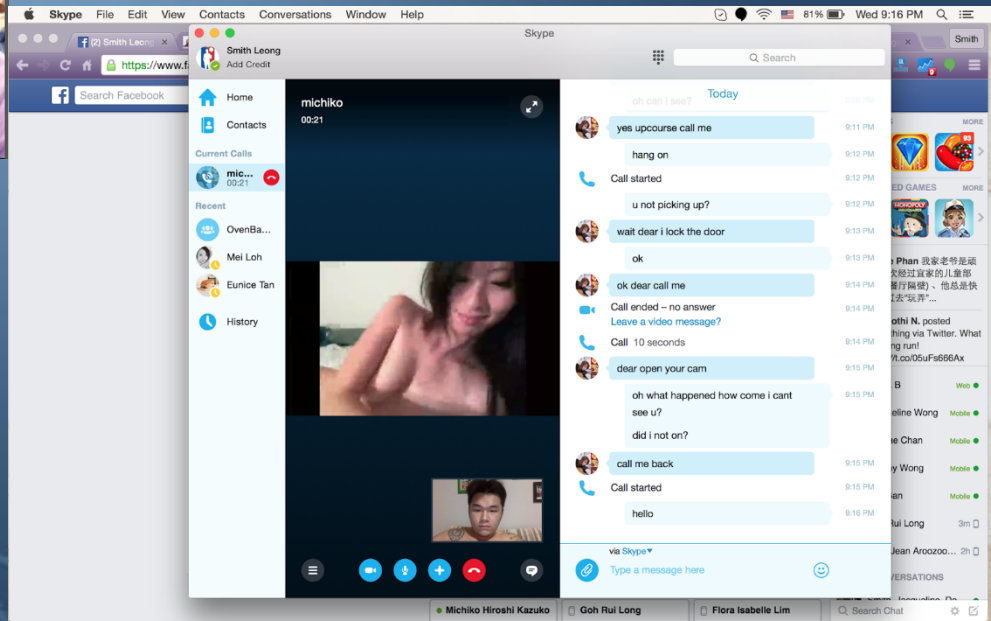

How a Botnet works
Infected Machine
(Bot/Zombie)
1
Infection
2
Connection
Cybercriminal
(Botmaster)
Malware
Distribution
Command &
Control Server (C2)
Spam
emails
Infected
websites
social media
posts
Botnet
4
Multiplication
3
Control

SEXTORTION

1. Approach by social media, such as FB

2. Ask a video chatting in nude

3. Ask the victim do something… masturbation etc, while they are using fake webcam program.



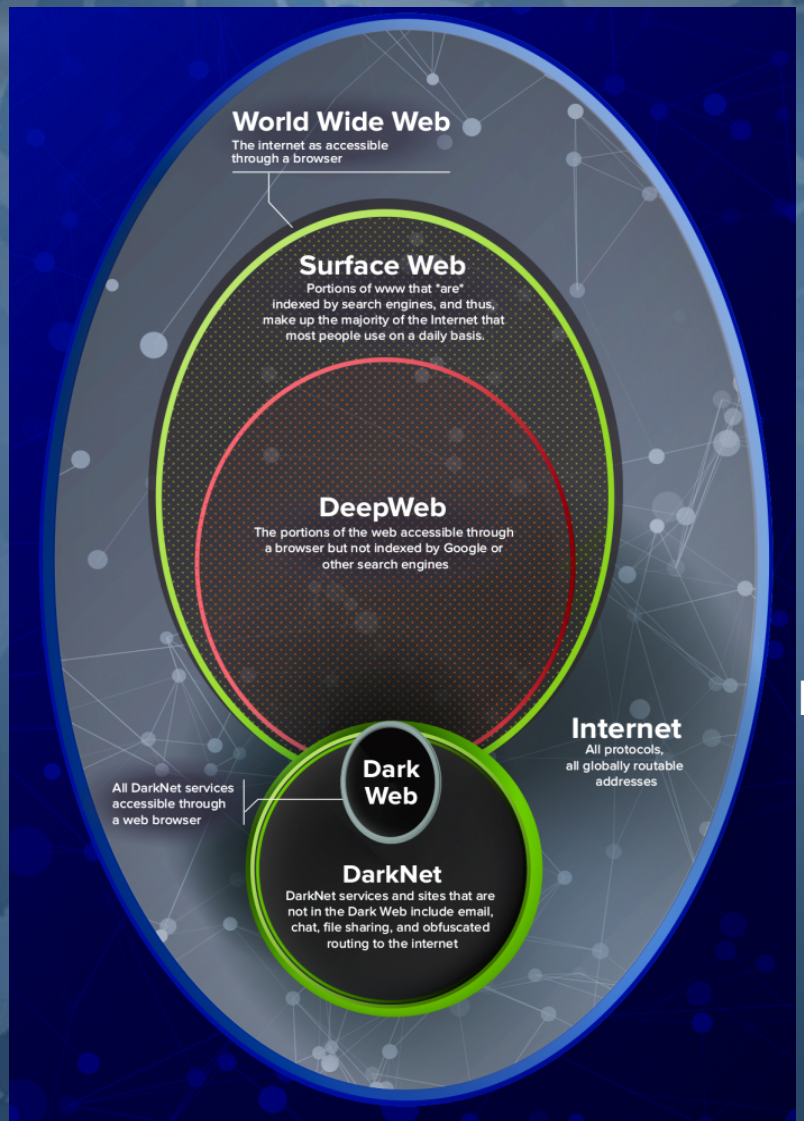
4. The criminals begin to demand a ransom.

Game-over..

DARKWEB AND BITCOINS

Crime as a service

Cybercrime as a service



Medical Record
Legal Documents
Drug Trafficking
Child Pornography
Private Communications
Hacking Groups
Rare Animal Trades
Particle Beam Weapons
Muderers/Hitman
FBI-Mid Classified Archives
Banned Media
Weapons
Ransomware

CRIME

Weapons

Terrorism

Counterfeit money

Human trafficking

Drugs

Thieves and burglars

Assassination services

New Life Identity

Human experiments

Money laundering

Supporter Abu Mustafa is able to raise five bitcoins (approx.. $1000) before his account was shut down by the FBI.

January 2015

Ali Shukri Amin used socilal media to instruct donors on the use of Bitcoin to provide untraceable financial support to ISIS.

June 2015

Mujahideen Shura Council in the Environs of Jerusalem receives around 0.929 bitcoins (approx.. $540) after adding the option of Bitcoin donation in June 2016.

July 2016

Bitcoin WARNING: ISIS using cryptocurrency to fund reign of terror as Bitcoin price soars

May 2015

Abu Ahmed al-Raqqa appeals to supporters of ISIS for donations in the form of bitcoins on the dark web.

August 2015

"Albanian Hacker" demands two bitcoins (aprox. $500) from an Ilinois internet retailer in exchange for removing bugs from its computer.

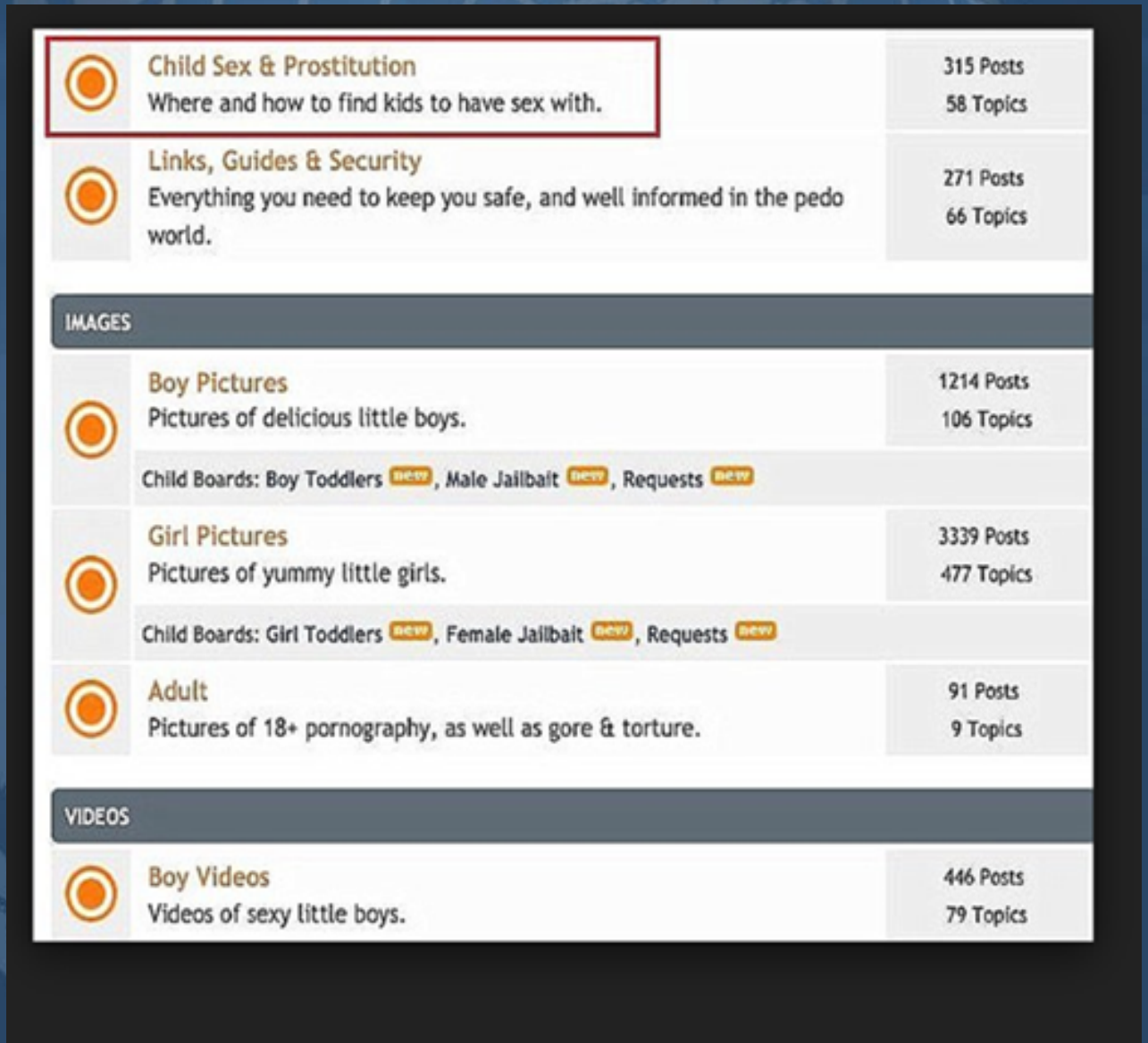
January 2017

Indonesia`s financial transactions agency announces that Bitcoin was used by IS to fund terrorist activities in Indonesia

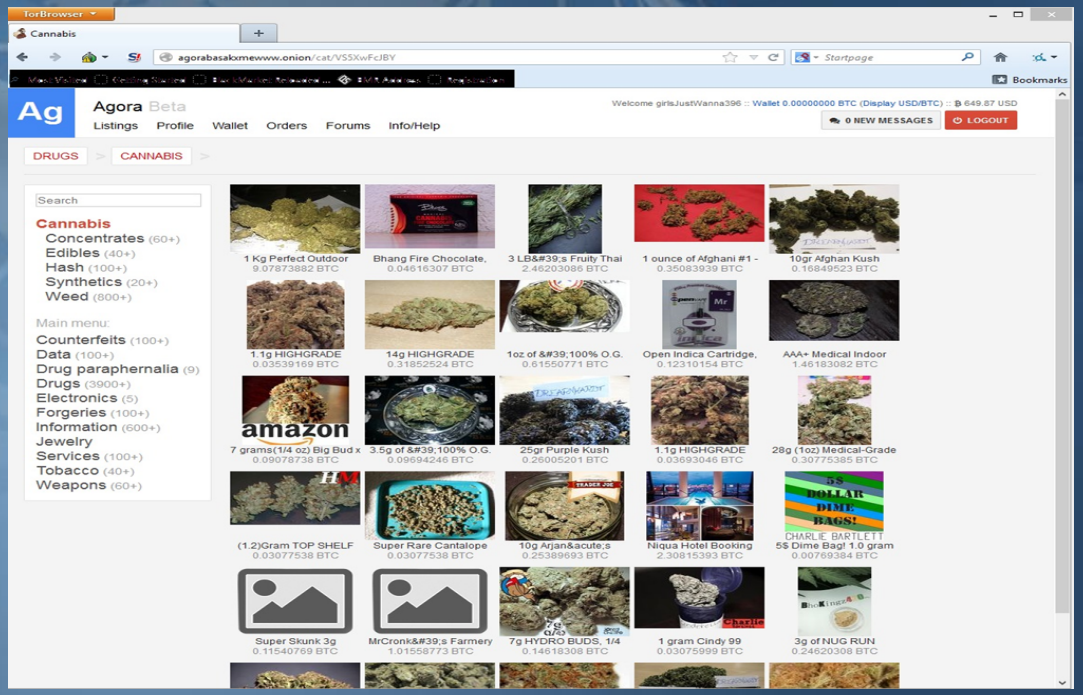
Bitcoin for Bombs

Bitcoin and other cryptocurrencies are gaining traction as a source of funding for terrorist groups, such as the self-proclaimed Islamic State. Counterterrorism policies should respond accordingly.

ONLINE CHILD SEXUAL EXPLOITATION



DARKNET MARKETS AND UNDERGROUND FORUMS



Van: darkface007@sigaint.org
Datum: 30-03-2016 20:25
Onderwerp: Die?

Hi . I'm darkface007 .
Bombing at the airport and metro station were succesful .

We will blow up airport again .
If you don't want to die no more people , you must pay 10 BTC to us .
Pay to 1HPFfCwrt6aRJeqtk37RzbMxG8xCJ52PrQ before 24h on April 1

darkface007

CHALLENGES FOR GOVERNMENTS

To Maintain a Safe and Secure Cyber Space in South East Asia

1

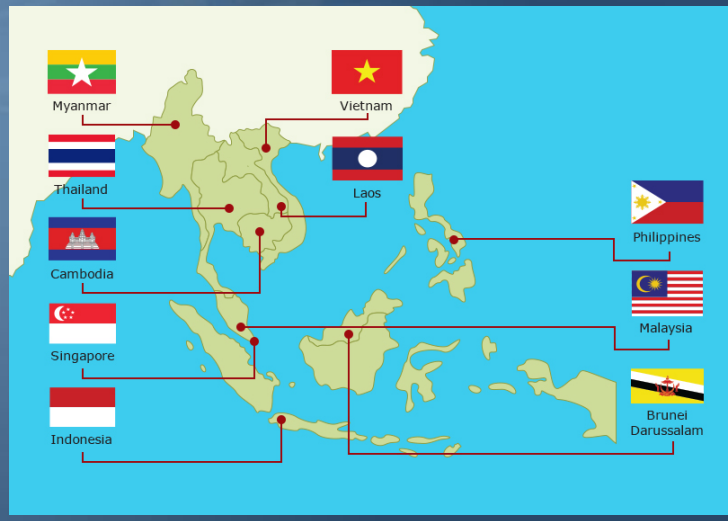
- Borderless nature of cybercrime
- Lack of awareness regarding cybercrime and overall cybersecurity among government officials
- Emerging Technology & Ease of Criminal Use

2

- General lack of properly trained specialized officers and equipment
- Lack of Proper Cyber Legislation
- Volume of crime
- Lack of Security within IoT Devices

3

- Capacity Building
- Difficulty in obtaining electronic evidence from foreign jurisdictions and ISPs
- Lack of International Co-Operation between agencies
- Staff retention issues

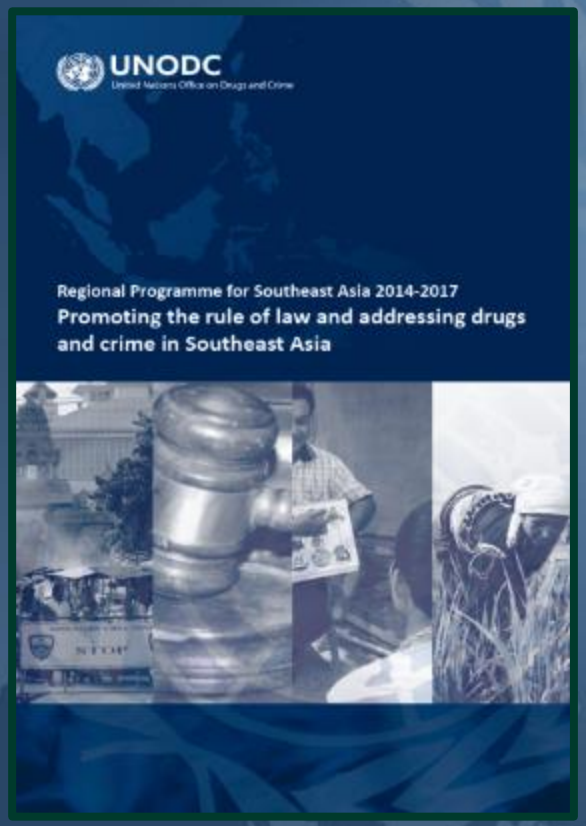


Presentation structure

- Background: Southeast Asia and regional integration
- Regional security and crime challenges
- Recommendations

UNODC Regional Programme for Southeast Asia

What is the Regional Programme?



UNODC Regional Programme for Southeast Asia

- The first integrated UN regional programme to address drugs, crime, and terrorism
- Rapid regional consolidation –to support frameworks and networks that align with national, sub-regional and regional responses, including those of ASEAN Community vision 2025
- Developed based on consultation and research on current and emerging drugs, crime and terrorism challenges

Thank you

Jeremy Douglas
Regional Representative
United Nations Office on Drugs and Crime
Regional Office for Southeast Asia and the Pacific
jeremy.douglas@unodc.org
http://www.unodc.org/southeastasiaandpacific/
@jdouglasSEA

Alexandru CACIULOIU
Cybercrime and Cryptocurrency Advisor
Programme Coordinator for Southeast Asia and Pacific
alexandru.caciuloiu@unodc.org
https://www.linkedin.com/in/alexandru-caciuloiu-22928543
@alex_c_unodc