



UNODC

United Nations Office on Drugs and Crime

Regional Office for Southeast Asia and the Pacific

Legislation and International Cooperation to protecting CNI

Alexandru Caciuloiu

Cybercrime and Cryptocurrency Advisor

UNODC Global Programme On Cybercrime

Safeguarding Critical National Infrastructure (CNI) – Risks and Opportunities



UNODC

United Nations Office on Drugs and Crime

**Regional Office for Southeast Asia
and the Pacific**

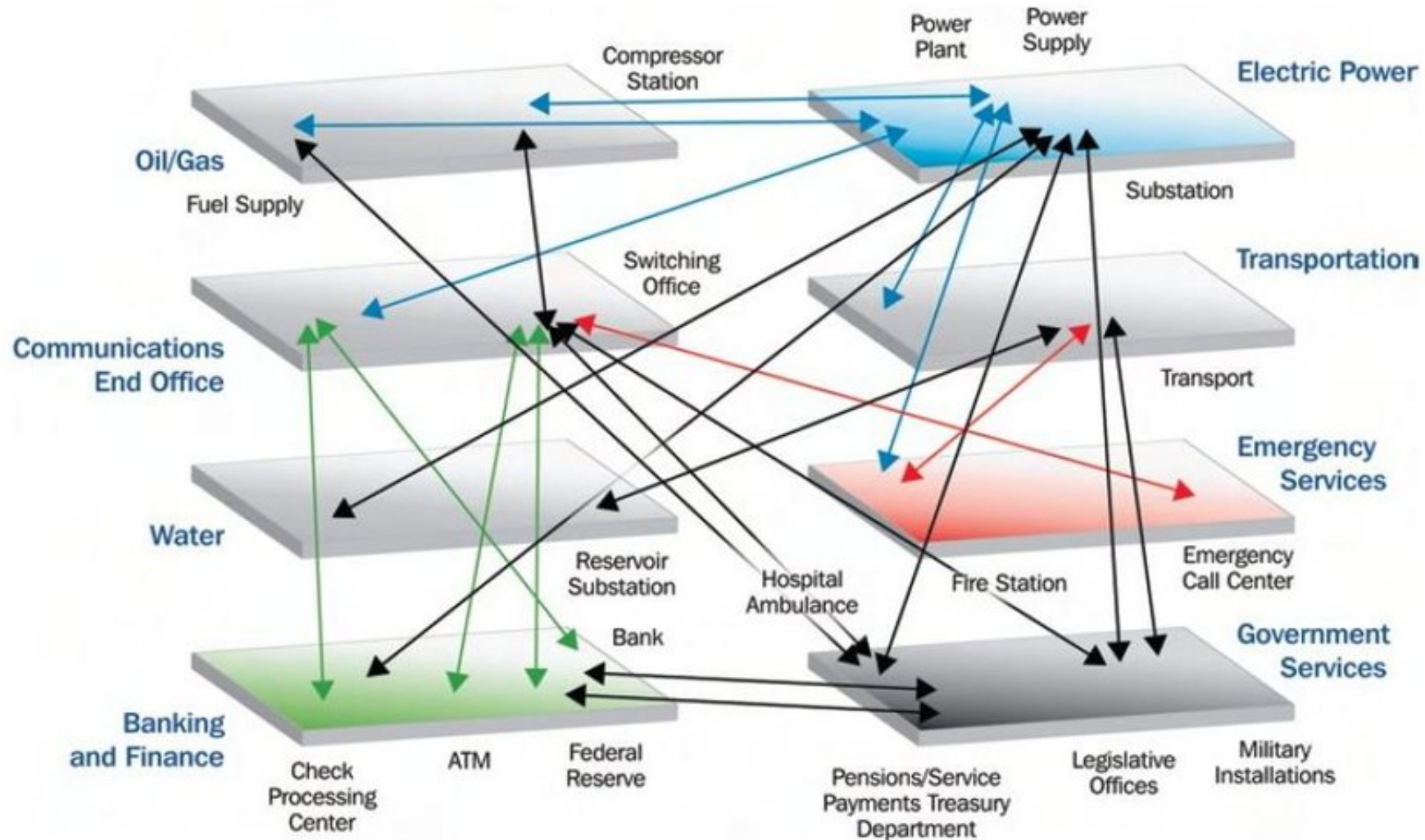


CNI at risk from the cyber domain


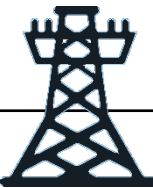












- Society relies on computerized system for almost everything in life
- The entire critical infrastructures is dependent on computerized systems (cyber physical systems)
 - Air, train and bus traffic control
 - Medical service coordination
 - Banking, Energy,
 - UxVs and Drones
 - Government and national security
- New type of battlefield for war and a new type of scene for terrorism



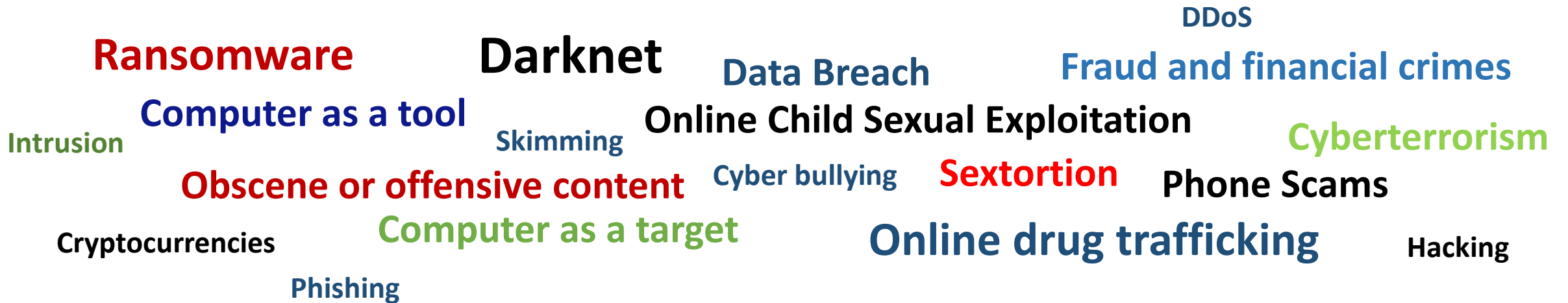
Interdependency of CNI



Threat Actors

Threat	Motivation	Target
Cyber espionage and State sponsored attacks 	Economical, political and/or military edge (advantages)	National interest cyber infrastructures State or commercial secrets Intellectual property (patents, etc.)  
Cyber Criminals 	Financial Gain	Financial or payment systems Personal private data Banking accounts and credentials Patient medical records    
Hacktivism 	Influencing political decision making or determining social change	State or commercial secrets Personal information regarding political decision makers   
Insider threat	Personal gain/advantages Revenge	State or commercial secrets Intellectual property Personal/private data  

what is *cybercrime*?



- Proper cybercrime legislation:
 - Subjective and procedural
 - Digital evidence
- Capacity building and strengthening
- International cooperation

- Countermeasures and the right to fight back(ethical hacker, cyberwarfare)
- **Can make the difference between protection of citizens and oppression**
- Internal aspects (rules between citizens of the same country)
- External aspects (rules between states)

National Protective Frameworks

- National legislation and Policy
 - Cybersecurity policies
 - Cybercrime laws
 - Digital evidence provisions
 - Procedural cybercriminal law
- Technical Protection
 - CERT/CIRT/CSERT
 - National/Government/Sectorial
 - Standards for organizations
- Criminal Justice System
 - Cybercrime Investigations Unit
 - Digital Forensics Lab
 - (Cybercrime)Prosecution
 - Specialized courts
- National Security/Intelligence
 - Early warning
 - Intelligence
 - **Counter-cyber operations**



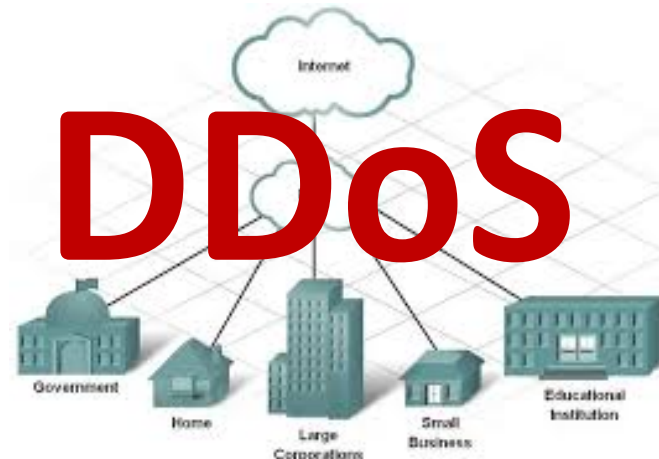
Court



CERT



Cybercrime Investigations Unit



ISP



Prosecutor



Digital Forensics Lab



International Frameworks

- Treaties/Conventions

- International Cyber Norms

voluntary norms of responsible state behavior during peacetime

- Interstate Cooperation
 - Multilateral agreements
 - Bilateral agreements

- International Technical Standards
 - ISO Standards (ISO27001)
 - HIPAA
 - NIST

Rules for States behaviour in *cyberspace*

When can we say that a state is responsible for cyber-attacks?

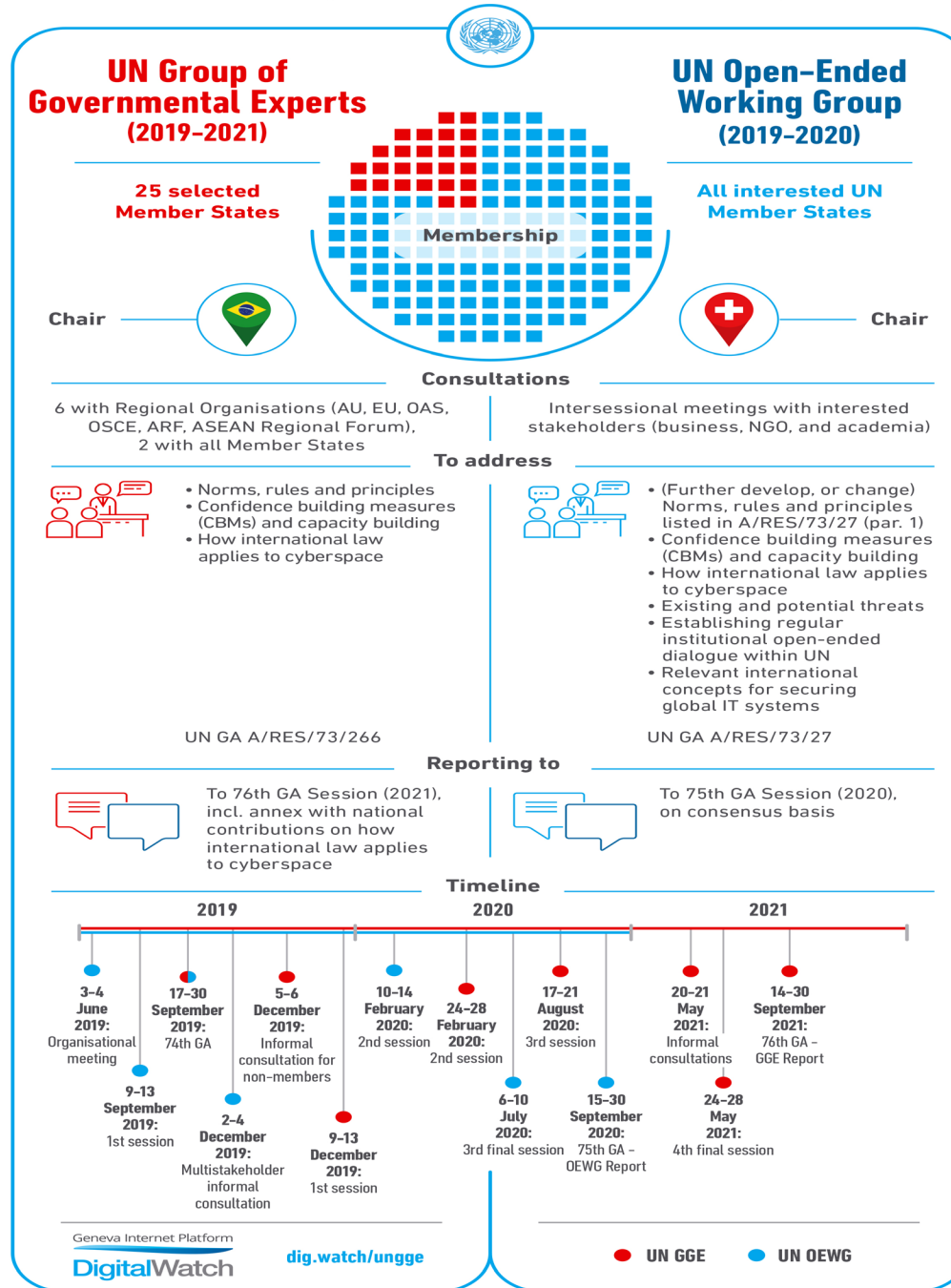
How can we qualify a cyber-attack under international law?

- 1. States can be held responsible for cyber-attacks, although proving their responsibility can be incredibly difficult.
- 2. A cyber-attack can easily be considered a violation of an international obligation, at least in terms of failing to take appropriate steps to stop the threat.

Three criteria have been identified for the **attribution** of responsibility to States

- a) **Effective control doctrine** recognizes a country's control over non-state actors only if the actors in question act in "complete dependence" on the State;
- b) **Overall control doctrine** held that a state is responsible where it has a role in organizing and coordinating the action and it has therefore an overall control over the group carrying out the attack;
- c) **Due diligence doctrine** which maintains that a state is also responsible when it fails to take appropriate steps, where those steps were evidently necessary, to avoid the violation of an international obligation.

The United Nations **Group of Governmental Experts (GGE)** on Advancing responsible State behavior in cyberspace in the context of international security (formerly: on Developments in the Field of Information and Telecommunications in the Context of International Security) is a UN-mandated working group in the field of information security. Six working groups have been established since 2004, including the GGE 2019-2021. The UN GGE can be credited with two major achievements outlining the global agenda and introducing the principle that international law applies to the digital space.



In 2018, another UN-mandated working group – the **Open-Ended Working Group** on Developments in the Field of ICTs in the Context of International Security (OEWG) – was established in parallel with the GGE, involving 'all interested states'.

UNITED NATIONS OFFICE ON DRUGS AND CRIME



Terrorism Prevention

**Mandated by the General Assembly to:
(reaffirmed in resolution 72/194 (2017))**

- ❖ Transport Terrorism Offences (aviation and maritime)
- ❖ Chemical, Biological, Radiological, and Nuclear Terrorism and Proliferation of WMDs by Non-State Actors
- ❖ Human Rights while Countering Terrorism
- ❖ Financing of Terrorism (incl. through virtual cryptocurrencies)
- ❖ Protection of Critical Infrastructure from Terrorist Attacks incl. Cyberattacks
- ❖ Use of the Internet/Social Media for Terrorist Purposes
- ❖ Foreign Terrorist Fighters
- ❖ Criminal Justice responses to Violent Extremism

GOAL:

To better equip governments to handle drugs, crime, terrorism, and corruption-related issues, by maximizing knowledge on these issues among governmental institutions and agencies, and also to maximizing awareness of said matters in public opinion, globally, nationally and at community level.

3 Pillars

- Field-based technical cooperation
- Research and analytical work
- Normative work to assist States in the ratification and implementation of the relevant international treaties and the development of domestic legislation

Global Programme on Cybercrime



Cybercrime



Online Child Protection



Digital Forensics

UNODC increases the capacity of ASEAN Member States to more effectively respond to the terrorists and FTFs in cyberspace



The regional exercise brought together officials from cybercrime agencies, computer emergency response teams (CERT), counter-terrorism agencies, police, and prosecutors from ASEAN Member States to practice responding effectively to the terrorist and FTF phenomenon

Bangkok (Thailand), 20 December 2019 - 35 officials from nine ASEAN Member States completed a four-day *Regional Exercise on Cyber Threat Intelligence Sharing to Respond to Terrorists and Foreign Terrorist Fighters (FTFs)*. The exercise was developed by UNODC's Global Programme on Cybercrime in collaboration with UNODC's Regional Office for Southeast Asia and the Pacific Terrorism Prevention Programme, and made possible with funding from the governments of Canada and Japan. The regional exercise marked an important milestone in regional collaboration in technical cyber operations to support investigation and prosecution of returning, relocating or transiting FTFs in Southeast Asia. As a result of the exercise skills of the officials were enhanced to gather and share intelligence, convert intelligence into evidence, collect evidence, and how to use secure and specialized cyber techniques to preserve the integrity and ensure admissibility of the digital evidence.

<https://www.unodc.org/southeastasiaandpacific/en/2019/11/cybercrime-terrorists/story.html>

UNODC hosts cyber threat intelligence in countering terrorist operations training in Lao PDR



Mr. Maithong Thammavongsa, Deputy Director of International Organization (Ministry of Foreign Affairs) delivers opening remarks at the training session

Vientiane, Lao PDR (14 November 2019) - Officials from the Lao government completed a three-day training course on darknet investigations and countering terrorist operations online. As a part of UNODC's Global Programme on Cybercrime, participants learned how to monitor criminal activity and collect cyber threat intelligence on the darknet. The training also helped build connections and develop relationships between Lao officials working to address cybercrime in Lao PDR, including law enforcement officers, prosecutors, and information technology experts from various departments across government.

<https://www.unodc.org/southeastasiaandpacific/en/laopdr/2019/11/cyber-crime/story.html>

UNODC engages ASEAN in regional exercise on cyber threat intelligence collaboration for joint cybercrime and counter terrorism response



Langkawi (Malaysia), 26 February 2019 - United Nations Office on Drugs and Crime, Regional Office for Southeast Asia and Pacific, has organized today the first of its kind, regional exercise focusing on cyber threat intelligence and coordinated regional/sub-regional response to cybercrime and terrorism through cyberspace. This initiative is part of UNODC's broader support to UN Member States in Southeast Asia to strengthen the capability and response to identify, investigate, and pursue cyber-criminals to counter terrorist use of information and communications technology.

<https://www.unodc.org/southeastasiaandpacific/en/2019/02/cybercrime/story.html>

Topics

- Alternative development
- Corruption
- Crime prevention and criminal justice
- Cybercrime
- Drug prevention, treatment and care
- Drug trafficking
- Firearms
- Falsified medical products
- HIV and AIDS
- Trafficking in persons and smuggling of migrants

Stories from UNODC

UNODC opens the first specialized Forensics Laboratory in Laos for analysing digital evidence



Vientiane (Lao PDR) 23 August 2019 -The United Nations Office on Drugs and Crime Global Programme on Cybercrime and the Lao People's Democratic Republic Police Force have jointly opened Laos' first Digital Forensics Laboratory. The lab will specialize in the analysis of digital evidence seized, or resulting from, criminal investigations in Laos including transnational organized crime, cybercrime and wildlife crime. [\[Read More\]](#)

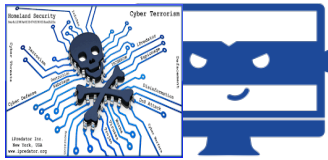


Ways Forward

- Support whole of government approach to countering cyber risks to CNI
- Foster cooperation on both national and international level between all stakeholders involved.
- Proper tools to report/detect/investigate and react to the cases encountered
- Deliver Programme that reduce the understanding gap between technical investigation on Cybercrime and threats to CNI
- Encourage creation of CSIRTs/CERTs in order to faster detect and respond to cybercrime
- Promote voluntary cooperation with the private sector in order to prosecute cyber-criminals
- Promote regional information exchange to identify, apprehend and prosecute cybercriminals

Reach out to UNODC- Global Programme on Cybercrime

Southeast Asia and Pacific Actions for 2020 - 2021



Cyber threats to CNI



National Cybercrime
Roundtable Discussion



Digital Forensics

Cryptocurrencies
Working Group

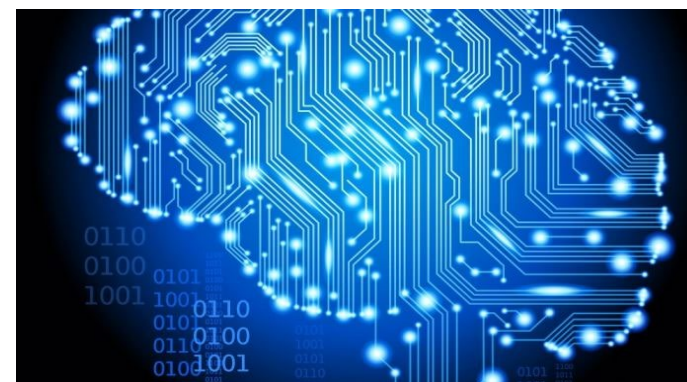


Regional Online Child Sexual
Exploitation Working Group



Ways forward?

Blockchain



Artificial Intelligence



Forensic-by-design

Time for a coordinated effort

National
Governments

International
Organizations

Industry



NGOs

Academia

Thank You

The UNODC Global Programme on Cybercrime

Alexandru CACIULOIU
Cybercrime Programme Coordinator (SE Asia and Pacific)

alexandru.caciuloiu@un.org

@alex_c_unodc