Combatting Cybercrime

CENTRAL ASIA REGIONAL EXPERT LEVEL WORKING GROUP ON DIGITAL TRADE

Tuesday, Sept 6 | Day 2

Keong Min Yoon, Counsel, World Bank

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

OVERVIEW

1. Development and Cybercrime
2. Building Cybercrime Framework
3. Legal Framework
4. International Cooperation
5. Public-Private Cooperation

1.DEVELOPMENT AND CYBERCRIME

Creating an enabling environment for the digital economy

INTRODUCTION

Cybercrime is a threat to the global economy as well as peace and security

- Governments must respond through effective training, adaptive legal frameworks, improved information sharing, and continuing public outreach programs

“Cyberspace” - a virtual world inseparable from the real, physical world

“Cybercrime” - criminal conduct in cyberspace directed against the confidentiality, integrity, and availability of data, technologies, and computer systems.

“Cybersecurity” - the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the availability, integrity, and confidentiality of assets in the connected infrastructures pertaining to government, private organizations and citizens.

GLOBAL CYBERCRIME TRENDS

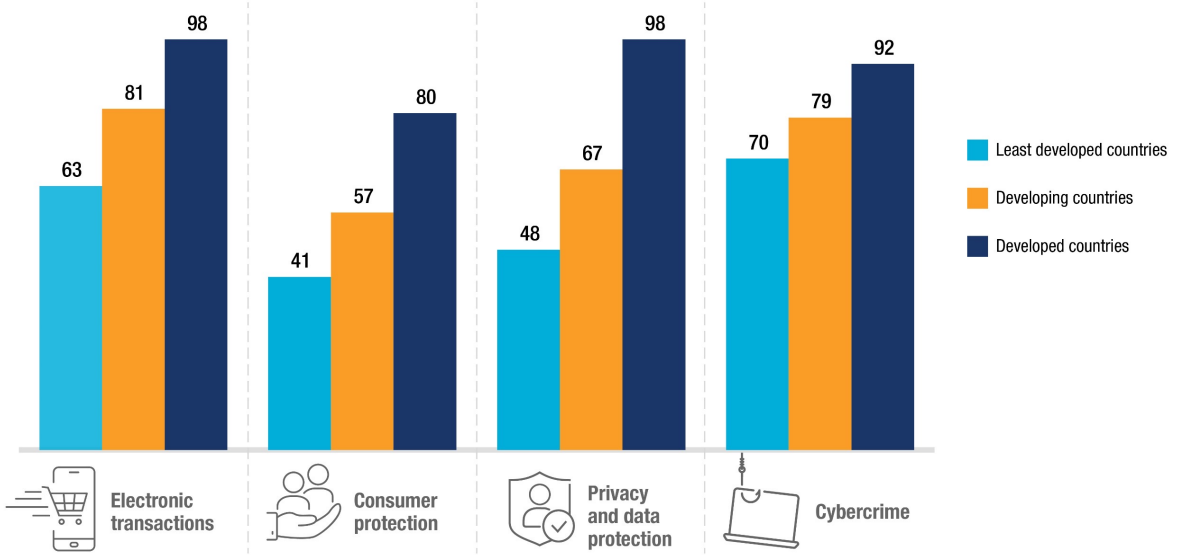
Cross-border data flow
- Cloud computing

Asset Recovery
- Cryptocurrency & darknet

Consumer Sensitivity & Focus on Human Rights
- Public-Private Cooperation

Emerging Technology
- AI, blockchain, IoT, etc.

Box D0.1: Cyberlaw Adoption in 2021 (Share of countries, percentage)



UNCTAD

DEVELOPMENT AND CYBERCRIME

The Internet has become an essential foundation for sustainable economic development

“Cyberspace” - a virtual world inseparable from the real, physical world

Information Communication Technologies (ICTs) play an integral role in maintaining and managing the society

- buildings, cars, aviation services, power supplies, etc.

Growing reliance on ICTs means more cyber threats, risks, and vulnerabilities

- *If unchecked, may result in vulnerabilities for* users, businesses, and *critical infrastructure*

DEVELOPMENT AND CYBERCRIME

Developing countries most vulnerable to cybercrime

- Needs capacity to combat cybercrime
- Growing and improving cybercriminals

https://policyaccelerator.uncdf.org/policy-tools/brief-cybersecurity-digital-economy

CYBERCRIME AND THE WORLD BANK

An international development institution established by its Articles of Agreement

- Reduce poverty, improve living conditions, and promote sustainable and comprehensive development around the world
- Provide financial assistance to countries for reconstruction after WWII

AAA-rated financial institution, with sovereign governments as shareholders

- With twin goals of ending extreme poverty & promoting shared prosperity

CYBERCRIME AND THE WORLD BANK

WB has been supporting developing countries in various sectors such as ICT, transportation, urban planning, energy, health, education and social protections.

- Notably, an overwhelming majority of the projects contain ICT components

Along with key partner organizations, WB offers a multidimensional approach

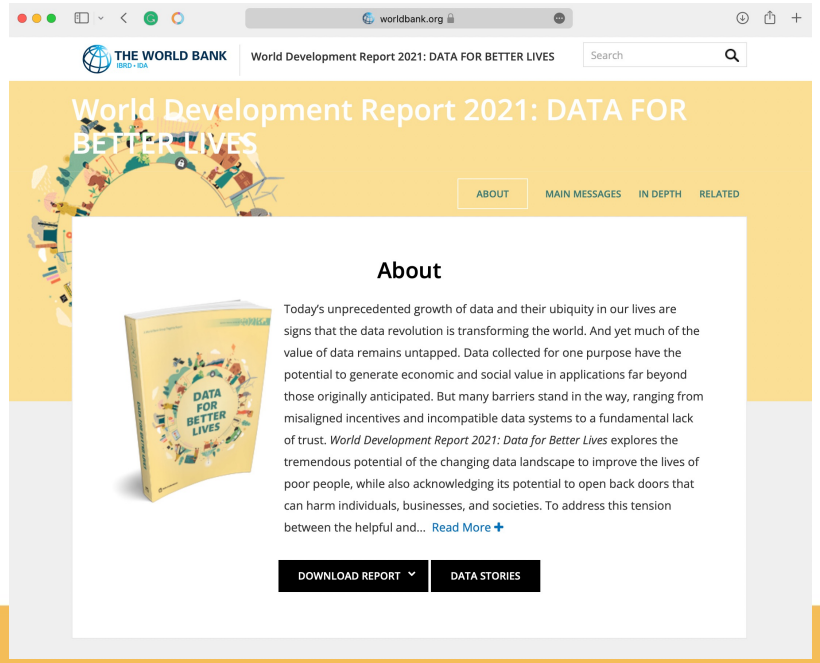
- a transnational cooperation among the sovereign states

Cybercrime and Digital Economy

Data policies, laws, and regulations: Creating a trust environment

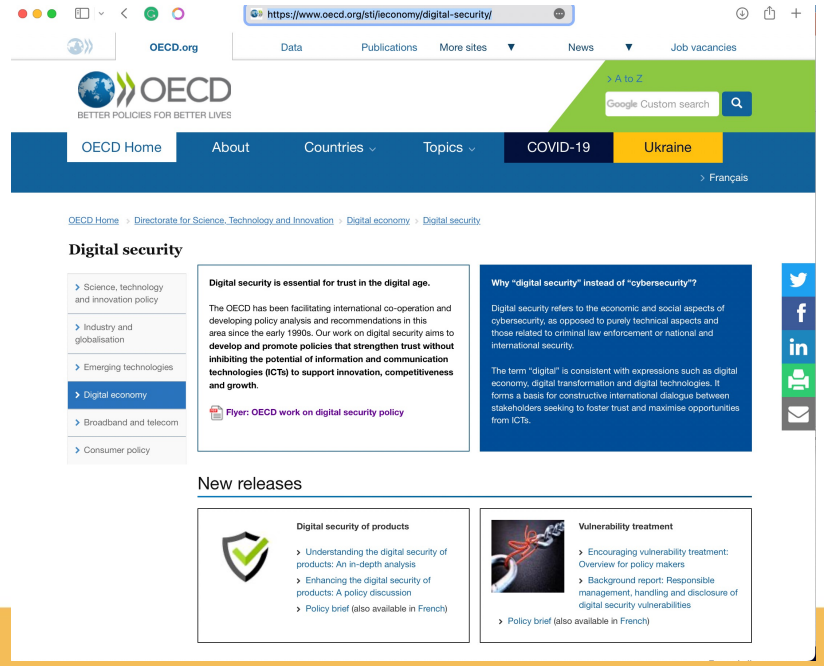
Main messages

1. Trust in data transactions is sustained by a robust legal and regulatory framework encompassing both *safeguards,* which prevent the misuse of data, and *enablers,* which facilitate access to and reuse of data.
2. Safeguards must differentiate between *personal data,* requiring a rights-based approach with individual protection, and *nonpersonal data,* allowing a balancing of interests in data reuse.
3. Enablers for data sharing are typically more developed for *public intent data,* where public policy and law mandating data access and sharing are more readily established, than for *private intent data,* where governments have more limited influence.
4. Creation of a trust environment remains a work in progress worldwide, especially in low-income countries. There is no one-size-fits-all legal and regulatory framework. In countries with weak regulatory environments, the design of suitable safeguards and enablers may have to be carefully adapted to local priorities and capacities.



https://www.worldbank.org/en/publication/wdr2021

OECD Digital Security



Effective digital security policies are essential for growth and well-being

The OECD provides a unique forum to develop and promote evidence-based policy analysis and advice to **strengthen security and trust, without inhibiting the benefits of the digital transformation** and its potential to increase well-being, innovation and growth. The OECD has been at the forefront of facilitating international co-operation on digital security policy since the 1990s. The OECD focuses on the economic and social aspects of cybersecurity, as opposed to aspects that are purely technical, directly related to criminal law enforcement or national security.

The OECD approach to digital security is grounded in **risk management** and focuses on **identifying the most effective policy tools** to address the economic and social challenges that often limit the ability of stakeholders to optimally manage digital security risk. These challenges include, for instance, a shortage of skills and talent, a lack of digital security innovation, unclear assignment of roles and responsibilities to economic actors, misaligned market incentives, information asymmetries as well as the cultural and legal barriers to effective co-operation across borders and stakeholder groups. OECD's work on digital security policy:

- Is carried out through the **Working Party on Security in the Digital Economy (SDE)**;
- Builds on the outcomes of the **Global Forum on Digital Security for Prosperity**; and
- Supports the development of **OECD Recommendations** on digital security policy.

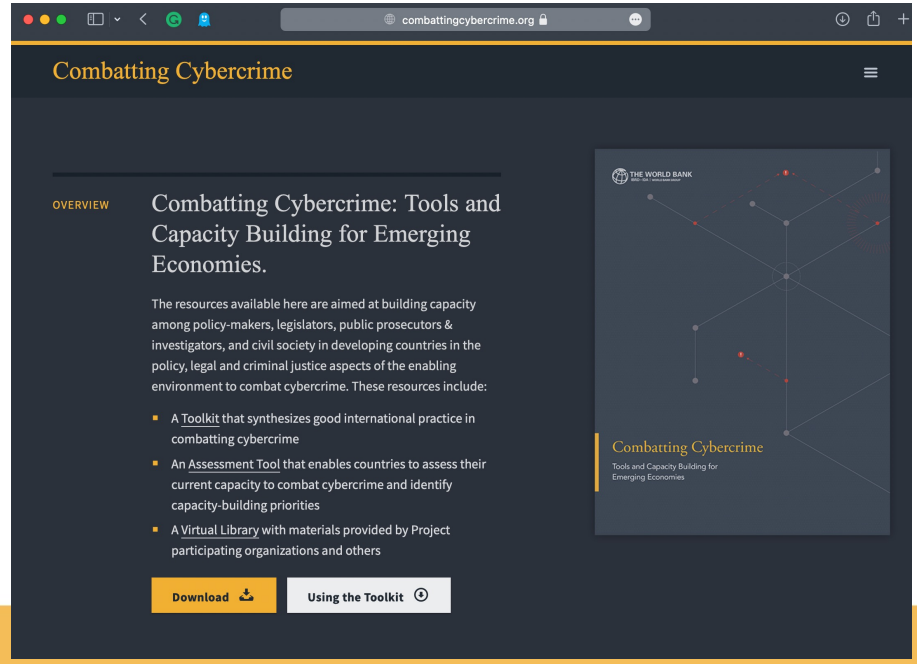
https://www.oecd.org/sti/ieconomy/digital-security/

THE WB COMBATTING CYBERCRIME PROJECT

Aims to enhance the capacity of policy-makers, legislators, judges, lawyers, prosecutors, investigators and civil society on various legal and non-legal issues that comprise the fight against cybercrime.

The Projects consists of four parts:

- Toolkit
  - Synthesizes good international practice in combatting cybercrimes and is organized in nine dimensions
- Training Material
  - Provides more concise explanation of nine dimensions with guidance, examples, cases, and emerging trends
- Assessment Tool
  - Enables countries to assess their current capacity to combat cybercrime and identify capacity-building priorities, and allocate scarce capacity-building resources
- Virtual Library
  - Offers materials provided by Project participating organizations



7 DIMENSIONS OF THE COMBATTING CYBERCRIME PROJECT

7 essential dimensions of combatting cybercrime

01. Policy Framework
02. Substantive Law
03. Procedural Law
04. Enabling Framework
05. Safeguards
06. International Cooperation
07. Capacity Building

LOGIC BEHIND THE SEVEN DIMENSIONS OF THE COMBATTING CYBERCRIME PROJECT

Countries beginning to combat cybercrime tend to focus on “criminalization” aspect

- However, there are other legal rules and non-legal systems that are also important and necessary.
  - Ex) A well-designed statutes of cybercrime laws cannot be enforced without sufficient resources to collect and analyze electronic evidence.

Synthesized expertise and experience of various organizations in the world & Categorized them into 7 dimensions:

- To successfully combat cybercrime, limited resources must be adequately distributed to each of the 7 dimensions
- Each dimension introduces concepts, examples, cases, and emerging trends as well as guidance on building capacity in each dimension

PARTNER ORGANIZATIONS

The Project's Partner Organizations

- Council of Europe (CoE)
- International Association of Penal Law (AIDP)
- Global Forum on Cyber Expertise (GFCE)
- International Telecommunication Union (ITU)
- INTERPOL
- Korea Supreme Prosecutors Office (KSPO)
- Oxford Cyber- security Capacity Building Centre (Oxford)
- United Nations Conference on Trade & Development (UNCTAD)
- United Nations Interregional Crime and Justice Research Institute (UNICRI)

Financed by a grant from the Korean Ministry of Strategy and Finance under the Korea-World Bank Group Partnership Facility (KWPF) Trust Fund

2. BUILDING CYBERCRIME FRAMEWORK

The first step to combatting cybercrime

RATIONALE & OBJECTIVES OF CYBERCRIME FRAMEWORK

Focus on strengthening the readiness of criminal justice actors to various forms of cybercrime

The data-heavy and transnational nature of cybercrime demands:

- Development of the capacity to not only deal with the electronic nature of cybercrime, but also its international dimension
  - Ex) Extraction, preservation and protection of e-evidence requires a specialized set of expertise
- Cooperation at all levels:
  - Public/private (in particular law enforcement/internet service provider),and international cooperation

START WITH POLICY FRAMEWORK

The 1st step to combat cybercrime

Key Elements

- Policy Instrument
  - National Cybersecurity Strategy (NCS)
- Institutional Governance
  - Central Cyber Coordination
  - Organizing & Coordinating Authorities

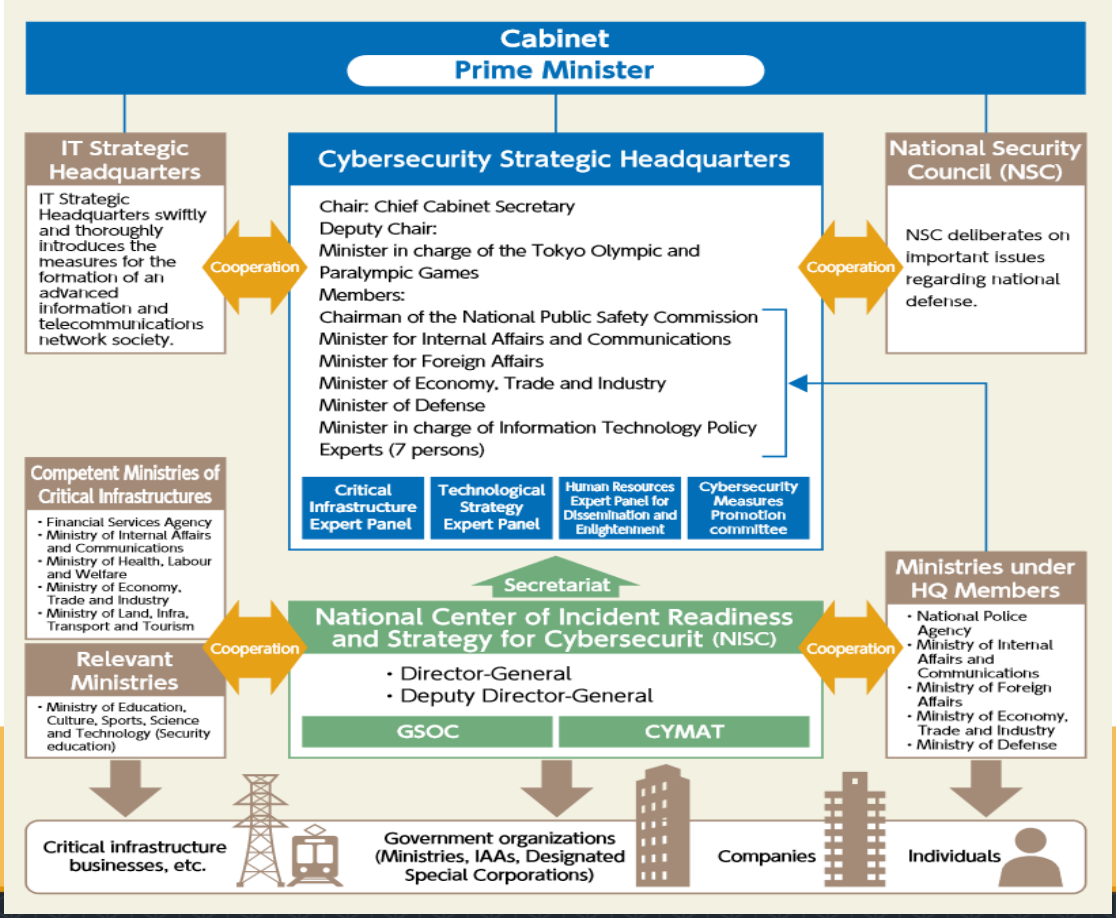
CASE STUDY: UK NCS 2016-2021

National Cyber Security Centre
a part of GCHQ

FOUR LARGE & BASIC GOALS

1. ***Tackling cybercrime***,
2. ***Increasing cyberattack resilience***
3. ***Helping shape and open-up cyberspace***
4. ***Eliminating silos***

INSTITUTIONAL GOVERNANCE: JAPAN'S INSTITUTIONAL FRAMEWORK FOR CYBERSECURITY



Central Cyber Coordination
- National Cyber Office
- Computer Incident Response Team (CIRT)

KOREA'S INSTITUTIONAL CYBERCRIME FRAMEWORK

Categories	Agencies in Charge	Relevant Statutes
Information Communications Policies	Ministry of Science, ICT and Future Planning Korea Communications Commission	Act on Promotion of Information and Communications Network Utilization and Information Protection Digital Signature Act Act on the Protection, Use, etc., of Location Information Telecommunications Business Act
Cybersecurity	Ministry of Science, ICT and Future Planning (for the private sector) KrCERT National Intelligence Service (for the public sector)	Act on the Protection of Information and Communications Infrastructure Act on Promotion of Information and Communications Network Utilization and Information Protection
User Protection	Ministry of Interior Korea Communications Commission Financial Services Commission	Personal Information Protection Act Act on Promotion of Information and Communications Network Utilization and Information Protection Special Act on Refund of Amount of Damage Caused by Telecommunications Bank Fraud
Cybercrime	National Police Agency Prosecutor's Office Ministry of Justice	Criminal Act Criminal Procedure Act Protection of Communications Secrets Act

KEY ELEMENTS OF CYBERCRIME POLICIES AND STRATEGIES

1. Engaged decision-makers
2. Synergistic cybersecurity strategies
3. Multi-stakeholder participation in strategy elaboration
4. Approaches support human rights and rule of law requirements
5. Cybercrime strategies require vertical and horizontal management
6. Concerted alignment of donor contributions and partner cooperation

3. LEGAL FRAMEWORK

Multidimensionality cybercrime law’s multidimensionality

INTERNATIONAL LEGAL TRENDS

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

2nd Protocol to Budapest Convention

Schrems II

Bilateral Agreements (U.S. Cloud Act)

LEGAL FRAMEWORK FOR CYBERCRIME

LAWS

- (1) governing behaviors in cyberspace &
- (2) establishing standardized procedures

Objective

- Global interoperability & harmonization of national laws

ROLE OF LEGAL FRAMEWORK

Creates sanctions for violations of laws;

Protects ICT owners and users by deterring harm to people, property, data, services, and infrastructure;

Recognizes and upholds human rights;

Permits the proper investigation and prosecution of specific crimes; and

Enables cooperation between countries in pursuing and punishing cybercriminals.

LIMITS OF TRADITIONAL CRIMINAL STATUTE

CANNOT always encompass the unique technological aspects of cybercrime

"[s]pecific and extensive cybercrime legislation will provide judicial consistency…as well as facilitate the enforcement of the law."

DEVELOPING CYBERCRIME-SPECIFIC LEGISLATION

A central part to developing a nation's capacity to combat cybercrime and furthering interoperability

Should be supported by other stakeholders, public and private, in the appropriate tailoring, targeting, and wording of any such legislation

FIVE DIMENSIONS OF LEGAL FRAMEWORK

1. Substantive law
2. Procedural law
3. e-Evidence law
4. Jurisdiction
5. Safeguards

CONDITIONS AND SAFEGUARDS UNDER ECHR

Conditions to be met when limiting rights Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)

Exclusive competence of the law (**legal basis**)

Need to pursue a legitimate aim (**legitimate aim**)

“Necessity of the interference in a democratic society”... which means that the interference must:

- Correspond to a "pressing social need“ (**necessity**)
- Be proportionate to the aim pursued (**proportionality**)

Requirements implied by the “necessity” and “proportionality” principles might be classified under the one or the other notion.

Source: Council of Europe (CoE)

LEGAL BASIS

Criminal statutes must be “accessible, clear, and predictable”

- “Known and predictable”

To bring charges against a defendant, there must be “a legal basis”

- A specific law or regulation, that publicly established and clearly defined the illegality of the underlying conduct

LEGITIMATE AIM

Prerequisite for a government to limit the exercise or expression of a person's fundamental rights.

"Legitimate aim" typically includes:

- Public safety
- Public health and morals
- Fostering the economic well-being of the community
- National security, and
- Guarding the rights of minorities and the most vulnerable members of a society.

US: STORED COMMUNICATIONS ACT (SCA)

The five instances when sufficiently compelling circumstances justify the government's secret intrusion into a person's private email account:

- (1) "Endangering the life or physical safety of an individual;"
- (2) "Flight from prosecution;"
- (3) "Destruction of or tampering with evidence;"
- (4) "Intimidation of potential witnesses;" and
- (5) "Seriously jeopardizing an investigation or unduly delaying a trial."

ADEQUACY

Safeguards must remain applicable to specific circumstances

- Considering the rights protected pursuant to the domestic and international legal obligations of a state
  - Both domestic and international obligations

BUDAPEST CONVENTION: ART. 15

Art. 15 Conditions & Safeguards

- Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

PROPORTIONALITY

Relationship between the objective to be achieved and the means used to achieve such objective.

- Investigative powers and procedures must remain “proportional” to the circumstances.

OVERCRIMINALIZATION

Excessive extension of criminal law to involve acts that are “inappropriately or not responsibly enforced by such measures”

- Ex) legislation of morality without an identifiable victim
- Ex) politically motivated statutes

NECESSITY

European Court of Human Rights:

- An interference is only acceptable if it is “necessary in a democratic society.”
  - The existence of a “pressing social need” and of “relevant and sufficient” reasons.

Ensuring that the impact of the powers and procedures upon the rights, responsibilities, and legitimate interests of engaged and third parties remain consistent with the public interest

JUDICIAL / INDEPENDENT SUPERVISION

Traditional safeguard in the rule of law

- “[E]ssential to the rule of law in any land is an independent judiciary, judges not under the thumb of other branches of Government, and therefore equipped to administer the law impartially.”

Ensuring the legality of laws and bolsters the legitimacy of government by permitting “individual judges…[to] base their decisions solely on the laws and the facts of individual cases.”

Judicial authorities = neutral and detached authorities

- Supervision over the scope and duration of a power or procedure
- Monitoring the integrity and compliance of procedures and powers

HARMONIZATION OF NATIONAL LAWS

The international harmonization and interoperability of domestic laws prevent cybercrime from safe haven.

- International harmonization of substantive law and procedural law
  - removes obstacles to global evidence collection and sharing
- Common procedural rules
  - ensure that electronic evidence gathered in one jurisdiction would satisfy the admissibility standards in another

Many nations' laws already contain provisions enabling more effective international cooperation.

4. INTERNATIONAL COOPERATION

Overcoming jurisdictional challenges

INTERNATIONAL COOPERATION

International cooperation is a crucial aspect of international peace and harmonization and supports

(i) Capacity building;

(ii) Exchange and sharing of information, experiences, training programs, research and technical knowledge, and best practices for investigation & prosecution of cybercrime; and

(iii) Technical and economic assistance

CHALLENGES POSED BY TRANSNATIONAL NATURE OF CYBERCRIME

Domestic law enforcement authorities cannot make advancements on criminal proceedings when the perpetrators as well as key evidence, witnesses, and victims exist outside their jurisdiction

THE DUAL CRIMINALITY PRINCIPLE

Requirement that the alleged act, subject to an official request for extradition or Mutual Legal Assistance (MLA) agreement, must also be defined as a criminal offense under the criminal law of both the state making the request and the state whose assistance is requested.

One of the biggest jurisdictional obstacles to investigating and prosecuting cybercrimes

Dual criminality “exists if the offense is a crime under both the requested and requesting party’s laws.”

Barriers:

- Harder than ever for jurisdictions to maintain current and uniform definitions of cybercrime offenses
- Often gaps between different jurisdictions, which may result in failure to extradite perpetrators

OVERCOMING CHALLENGES POSED BY TRANSNATIONAL NATURE OF CYBERCRIME

1. Formal International Cooperation
   - Multilateral treaties on cybercrime, mutual legal assistance treaties, and extradition treaties
2. Informal International Cooperation
   - Different modalities of cooperation that is typically more hands-on, practical, and personal and conducted at an operational level between governments

THREE OBJECTIVES OF ESTABLISHING FORMAL INTERNATIONAL COOPERATION

1. Gap-fill national criminal laws against transnational cybercrime;

2. Proffer procedural powers where nations are not appropriately equipped to combat cybercrime; and

3. Create enforceable MLA provisions that would facilitate and expedite sharing and assistance in cybercrime matters

GLOBAL LANDSCAPE OF FORMAL INTERNATIONAL COOPERATION

Globally, more than eighty states have signed and/or ratified one or more binding cybercrime instruments, and many of those states have national cybercrime legislation

- (A) Multilateral treaties

In addition to multilateral treaties, countries have signed bilateral treaties and agreements directly

- (B) Mutual Legal Assistance Treaties (MLATs)
- (C) Extradition treaties
- (D) Cloud Act Agreements

MULTILATERAL TREATIES ON CYBERCRIME

a. BUDAPEST CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION) of 2001
b. COMMONWEALTH OF INDEPENDENT STATES (CIS) AGREEMENT
c. SHANGHAI COOPERATION ORGANIZATION (SCO) AGREEMENT
d. LEAGUE OF ARAB STATES CONVENTION ON COMBATTING INFORMATION TECHNOLOGY OFFENCES (ARAB CONVENTION)
e. AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION (AU CONVENTION)
f. UN TREATY ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

THE ROLE OF MULTILATERAL TREATIES ON CYBERCRIME

Harmonize national laws

Develop cybercrime investigative capacities

Promote and enhance international cooperation

Provide guidance to signatories on implementing national measures

Serve as a mutual legal assistance treaty for those states that do not already have an agreement in place with a state party in need of assistance

BUDAPEST CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION) of 2001

Foremost international instrument on cybercrime

- Open to signature by non-Council of Europe (CoE) Member States

Offers a guideline for Member States to create and harmonize their national legislation on cybercrime

Legally binding on its Member States

Clear definition of criminal offenses as balanced against procedural Safeguards

Accession of non-CoE Member States is restricted to those “invited” upon the unanimous consent of the Contracting Parties to the Convention

BUDAPEST CONVENTION'S MLA PROVISIONS

Obliges Parties to ensure that that procedural tools are available to investigate the enumerated crimes, as well as other crimes not listed in the Convention.

- Recognition of the importance of electronic investigations in any type of crime and at any stage of development.
  - Ex) Mobile-phone data
- The Convention's procedural tools are tailored to avoid violations of sovereignty and human rights while still enabling states to adequately investigate crimes.

Makes significant strides towards improving the timeliness with which cybercriminal matters are addressed between Parties.

- Requiring each state to create a "24/7 Network"

SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION (2nd PROTOCOL)

Addresses the challenges by providing greater international cooperation, focusing on 4 key elements:

- Measures to improve international cooperation between law enforcement and judicial authorities – including on legal assistance between authorities (“mutual legal assistance”);
- Cooperation between authorities and service providers in other countries;
- Conditions and safeguards for access to information by authorities in other countries; and
- Other safeguards, including data protection requirements

AREAS OF IMPROVEMENTS FOR FORMAL INTERNATIONAL AGREEMENTS

Inclusion

Multistakeholderism

Incorporating lessons learned

Overcoming persistent limitations in coverage

National implementation

International instruments aggravate differences among states

Safeguards

PLACE FOR INFORMAL COOPERATION

Informal mechanisms of international cooperation are essential to fill gaps that may not be addressed through formal mechanisms

Governments, international organizations and non-governmental organizations (NGOs) alike have all proposed various options supporting international interoperability

- Ex) UN General Assembly's adoption of a resolution dealing with computer crime legislation (1990)
- Ex) G8's release of a Ministers' Communiqué that included an action plan and principles for combatting cybercrime and protecting data and systems from unauthorized impairment (1997)
- Ex) World Summit on the Information Society (WSIS)'s issuance of the Geneva Declaration of Principles and Plan of Action (2003)

The US Department of Justice (DoJ) uses the term "operational police-to-police cooperation" rather than "informal cooperation" in order to underline that this cooperation is authorized under domestic law

INFORMAL COOPERATION MECHANISMS

Various forms and practices of “informal” international cooperation in the context of cybercrime include:

- 24/7 networks
- Information sharing & coordination centers
- Inter-institutional collaboration
- Private-public cooperation

24/7 NETWORKS

Designated directly reachable point-persons for every hour of every day, with contact information kept current.

For 24/7 networks to operate effectively, national point-persons must understand:

- Their own legal and policy framework;
- How their domestic arrangements intersect and interact with the larger international systems function;
- Have the minimum technical knowledge to understand cybercriminal behavior;
- Must be capable of communicating in foreign languages, with English language skills being a minimum.

BUDAPEST CONVENTION 24/7 HIGH TECH CRIME POINTS OF CONTACT NETWORK

Requires Parties to create a 24/7 High Tech Crime Points of Contact Network

Parties are required to

> "designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

5. PUBLIC PRIVATE COOPERATION

Working with the private sector

PUBLIC PRIVATE COOPERATION

Private sector holds most of e-evidence

- Majority of cyber infrastructure owned by the private sector

Shared responsibility- need a unified approach between the public and private sectors

Continuous process, with room for improvement

- Emerging threats: IoT

PRINCIPLES FOR ENHANCING EFFECTIVE COOPERATION

Principle 1: Embracing a shared narrative for collective action against cybercrime – A shared narrative is needed in order to appropriately engage, enable and empower all the actors and stakeholders.

Principle 2: Cooperating on the basis of long-term strategic alignment – Combatting cybercrime and securing cyberspace is a long-term endeavor that requires sustained commitment to finding common ground for cooperation, based on a periodically updated and improved understanding of each stakeholder's respective needs, goals and values.

Principle 3: Undertaking trust-building behaviors –Before even coming together to explore possible points of cooperation, it is important that actors work independently and on their own to establish themselves as responsible cyber-denizens.

Principle 4: Systematizing the cooperation – Cooperation should be institutionally anchored, while allowing space for personal connections to grow. Building the cooperation on institutional relationships will help to ensure continuity by making sure that successors are able to step into the cooperation and the role as fluidly as possible.

Principle 5: Ensuring value for participating in the cooperation – Mutual recognition of efforts and inputs helps capture value, as well as to solicit greater understanding about expectations.

Principle 6: Respecting concerns and challenges – The public-private cooperative effort should not be construed as a legal or contractual obligation, but, rather, as one developed on the basis of consensus.

https://www.weforum.org/projects/partnership-against-cybercrime

TYPES OF COOPERATION

Compulsory Cooperation → Voluntary Cooperation

Source: Council of Europe (CoE)

COMPULSORY COOPERATION

Required by legal instruments such as mutual legal assistance treaties and relevant domestic legislation

- Ex. CLOUD Act

Mutual Legal Assistance through government authorities

Requested States enforce MLA requests through their own domestic measures

Source: Council of Europe (CoE)

US: THE CLOUD ACT

The CLOUD Act of the United States

- Allowing the US to enter into negotiations for executive agreements with other nations that meet certain criteria to facilitate cross-border data sharing directly between US companies and foreign governments.
- For investigations of serious crime, CLOUD agreements can help remove restrictions under each nation's laws so that CSPs can comply with qualifying, lawful orders for electronic data issued by the other country.

VOLUNTARY COOPERATION

Direct cooperation with foreign service providers

Subscriber information sought from US companies

- US companies have their own policies
- Requirements depends on data type

BARRIERS TO COOPERATION

Complexity of Cross-border data restrictions

Beyond *legality* of sharing information, what about the ability (of gov't) to protect that information

Reputational damage in sharing (loss of competitive advantage)

Concern for liability as consequence of cooperation

Key Consideration: Law Enforcement and National Security

1. Essential guarantees in third countries for law enforcement and national security access to limit interferences to fundamental rights
2. Standard:
    1. Processing should be based on clear, precise and accessible rules (legal basis)
    2. Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated
    3. The processing has to be subject to independent oversight
    4. Effective remedies need to be available to the individuals

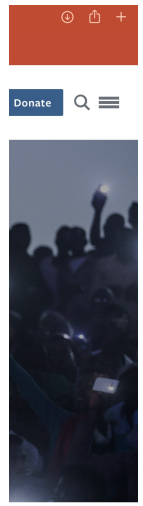
Challenges to Public-Private Cooperation

Viewing: Global Freedom Scores | **Internet Freedom Scores** | Democracy Scores

Quick Find: Country Name

Establishi
- private
  workinç
  actual i
- private
  consequ
  cyber-ir
- "trust"-
  governr
  busines
- Lack of
- scaling
  mid-size
  proprie

Country	Total Score and Status	Obstacles to Access	Limits on Content	Violations of User Rights
Iceland	96 Free	25	34	37
Estonia	94 Free	25	32	37
Canada	87 Free	23	32	32
Costa Rica	87 Free	20	33	34
Taiwan	80 Free	24	31	25
Germany	79 Free	22	29	28



rnet aking ilding. The es a ranked,

THE END