INTERPOL

National Cybercrime Strategy Guidebook

Japan-ASEAN Cooperation

April 2021

Foreword

As information technology becomes more embedded in our society, cybercrime has become a common hazard on a global scale. With more than 4.5 billion people online, half of the world's population is potentially at risk of falling victim to cybercrime.

The COVID-19 pandemic has resulted in the accelerated merging of our physical and cyber spaces and increased reliance on connectivity for many of our basic tasks, in both our work and personal lives.

An increasingly complex cybercrime landscape combined with the inherent challenges of cross-border investigations has placed additional strain on global law enforcement.

While the private sector has been transforming itself, the public sector continues to face challenges posed by a lack of information, strategies, resources, infrastructure and partnerships.

It is important for law enforcement to acknowledge that the current measures, practices and policies may not be enough to address today's ever-evolving cybercrime and identify what steps need to be taken to meet this shortfall.

The public sector must ramp up its preparedness, effectiveness and leadership for collective cyber resilience. Cybersecurity is both a shared responsibility and a common goal that we must constantly work towards.

When techniques and tactics are being replicated in attacks on different sectors around the world, this is where the true value of INTERPOL's global platform to help investigators exchange information securely and react rapidly, can be fully appreciated.

As part of these efforts to support our member countries, I am proud to present the **INTERPOL National Cybercrime Strategy Guidebook**.

The world is getting more and more connected and INTERPOL will continue to play a central and unique role as part of the global law enforcement community in our joint fight against cybercrime.

Jürgen Stock

INTERPOL Secretary General

Introduction

We have entered a paradigm where cyber and physical spaces merge, and digital transformation has increased our reliance on connectivity.

Law enforcement around the world has witnessed first-hand the unique criminal aspects the COVID-19 pandemic was breeding, especially the diversifying and growing impact of cybercrime. This phenomenon has made us rethink our global response and repurpose our global law enforcement network.

An August 2020 INTERPOL report which studied the impact of the coronavirus pandemic on the global cyberthreat landscape identified national cybercrime strategies as a way to build resilience of national infrastructure and services, helping countries counter cyberthreats effectively and protect communities from cyberattacks during the pandemic and beyond.

Under the mandate of "reducing the global impact of cybercrime and protecting communities for a safer world", INTERPOL Cybercrime Directorate delivers policing capabilities for tackling cybercrime. One of its primary objectives is to strengthen and enhance the capabilities of member countries in order to prevent, detect and investigate cybercrime.

This Guidebook provides INTERPOL member countries with a valuable resource for developing or updating their national Cybercrime Strategy. It helps gain insight into their current response to cybercrime and provides a means to design a more robust strategy and programme to overcome challenges that are hindering a more effective cybercrime response.

I recommend this Guidebook to our member countries to make their countries more resilient and agile in this highly digitalized world to effectively fight cybercrime.

Craig Jones

Director Cybercrime

Table of Contents

Acronyms

ASEAN Association of Southeast Asian Nations

ACCDP ASEAN Cyber Capacity Development Project

CERT Computer Emergency Response Team

CSIRT Computer Security Incident Response Team

DDoS distributed denial-of-service

Europol European Union Agency for Law Enforcement Cooperation

ICT information and communications technology

IoT Internet of Things

IP Internet Protocol

ITU International Telecommunication Union

MLAT mutual legal assistance treaties

SMART Specific, Measurable, Achievable, Relevant, and Time-Bound

UNODC United Nations Office on Drugs and Crime

Authors

Shane Cross, Simon Hirrle – INTERPOL

May-Ann Lim - TRPC Pte Ltd

Acknowledgments

This Guidebook was made possible by the efforts of numerous people throughout the various stages of its development. Several consultations, workshops, peer reviews and contribution meetings were held and the ASEAN Cyber Capacity Development Project (ACCDP) would like to thank the following people involved at the various stages of the Guidebook's development for their contribution:

- Steve Honiss – Aardwolf Consulting Ltd
- Benjamin Ang - S. Rajaratnam School of International Studies, Nanyang Technological University
- Claire Pluckrose
- Anthony Teelucksingh - United States Department of Justice
- Aysha Ahmed Bin Haji - Ministry of Interior of Bahrain
- Jeannie Tsang et al - Hong Kong Police Force
- Dr. Cristos Velasco
- Yoichi Kumota - National Center of Incident Readiness and Strategy for Cybersecurity, Japan
- Ismamuradi Abdul Kadir – Cybersecurity Malaysia
- ASEAN country representatives at the ACCDP Kick-off Workshop
- Dong Uk Kim, Pei Ling Lee, Wei Xian Tee - INTERPOL

Legal Notice

The Cybercrime Strategy Template included in the Guidebook is provided for educational purposes and as an example/suggestion for consideration only. It is not in any manner binding nor endorsed as an effective strategy by INTERPOL. Its adoption is at the discretion of the reader, and must be considered subject to applicable policies, laws and circumstances in the country concerned. INTERPOL shall not be liable for any damages or harm arising out of its adoption in any jurisdictions.

Copyright Notice

1. Introduction

Background

This Guidebook has been produced as part of phase two of the ASEAN Cyber Capacity Development Project (ACCDP II). The ACCDP is a project that is funded by the Japan-ASEAN Integration Fund (JAIF) 2.0 via the ASEAN Secretariat and with the Singapore Ministry of Home Affairs as the project proponent. INTERPOL is the implementing agency.

This project aims to strengthen the ability of countries to combat cybercrime and work together as a region and internationally. The ACCDP specifically addresses the need for criminal justice authorities to develop their cyberskills, knowledge and regional partnerships through tailored activities and products.

The ACCDP forms part of INTERPOL's global cybercrime response and supports the implementation of its global cybercrime strategy. INTERPOL supports national efforts to combat cybercrime and considers it a global focus area alongside terrorism and organized crime.

Methodology and approach in the development of the Guidebook

The consolidated findings of in-country assessments (National Cyber Reviews) conducted in the first phase of the ACCDP revealed that there was a clear need in many ASEAN member states (AMS) for a cybercrime strategy. Thus in phase two of ACCDP this Guidebook was developed.

The development of the Guidebook started with a one-week workshop attended by representatives from law enforcement, national cyber agencies and external advisors and continued with the input of various experts from INTERPOL and its member countries.

The information contained in this Guidebook is not tailored to any specific region but instead details identified good practices which are in use internationally.

Purpose of the Guidebook

The Guidebook is designed to be used by any country looking to develop, review or enhance its national cybercrime strategy.

The project observed a significant disparity between the anti-cybercrime initiatives, laws and processes in force in INTERPOL member countries and underlined the importance of more closely aligning them with international good practices.

This Guidebook was created to provide a methodological approach to the potentially challenging task of creating or updating a cybercrime strategy.

2. Cybercrime and Cybersecurity

2.1 The challenge of defining cybercrime

There is no universally accepted definition of cybercrime. The most common approach is to define the key terms used in cybercrime investigations. Examining frequently-used definitions will allow us to identify key concepts and use those definitions consistently in a country's cybercrime strategy.

One example of this approach is the Commonwealth's 2017 Model Law on Computer and Computer Related Crime ("Commonwealth Model Law")[1]. This law begins by defining some key terms: "computer data", "computer data storage medium", "service provider", and "traffic data". Following these definitions of key terms, the Commonwealth Model Law then identifies the core offences which it considers to fall within the scope of cybercrime – (1) illegal access, (2) interfering with data, (3) interfering with computer systems, (4) illegal interception of data, (5) illegal devices and (6) child pornography.

This approach is very similar to the Convention on Cybercrime of the Council of Europe (the Budapest Convention)[2], which contains initial definitions for "computer system", "computer data", "service provider", and "traffic data". The Convention then defines four categories of offences committed by means of computer systems and information technology. These categories are:

- Title 1: Offences against the confidentiality, integrity and availability of computer data and systems – illegal access, illegal interception, data interference, system interference, and misuse of devices;
- Title 2: Computer-related offences – computer-related forgery, computer-related fraud;
- Title 3: Content-related offences – child pornography;
- Title 4: Offences related to infringements of copyright and related rights;
- Title 5: Ancillary liability and sanctions – attempt and aiding or abetting, corporate liability.

Table 1: Comparison of Key Cybercrime Terms

Defined Term	Commonwealth Model Law	Budapest Convention
Computer data	"Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.	"Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.
Computer data storage medium	"Computer data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device.	(does not define this term)
Computer system	"Computer system" means a device or a group of inter-connected or related devices, including the internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function;	"Computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.
Service provider	"Service provider" means: (a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and (b) any other entity that processes or stores computer data on behalf of that entity or those users.	"Service provider" means: (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.
Traffic data	"Traffic data" means computer data: (a) that relates to a communication by means of a computer system; and (b) is generated by a computer system that is part of the chain of communication; and (c) shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.	"Traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

[1] https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf
[2] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Positive outcomes to cybercrime investigations can be contingent upon the successful collection, analysis and attribution of digital evidence. The term 'digital evidence' is used interchangeably with electronic evidence or e-evidence and refers to information and data that is stored on, received or transmitted by an electronic device. This includes evidence from digital devices or records obtained from online service providers.

2.2 Cyber-dependent crime vs cyber-enabled crime

In addition to defining key terms related to cybercrime - which can be a broad term covering a multitude of offences - it is important to differentiate between 'cyber-dependent crime', also referred to as 'pure cybercrime' and 'cyber-enabled crime'. The United Kingdom Home Office's series of research and analysis documents entitled "Cybercrime: a review of the evidence[3]" provides a useful reference and the following distinction is made between the two concepts:

- 'Cyber-dependent crimes' (or 'pure' cybercrimes) are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). These acts include the spread of viruses or other malware, hacking and distributed denial-of-service (DDoS) attacks. They are activities primarily directed against computers or network resources, although there may be a variety of secondary outcomes from the attacks. For example, data gathered by hacking into an e-mail account may subsequently be used to commit a fraud[4].
- 'Cyber-enabled crimes' are traditional crimes, which can be increased in scale or reach by use of computers, computer networks or other forms of ICT. Unlike cyber-dependent crimes, which solely rely on ICT, the underlying crimes of cyber-enabled crimes can be committed without the use of ICT. Two of the most pervasive types of cyber-enabled crimes are fraud and theft[5]. An example of this is scam e-mails that try to trick the recipients into transferring money to an unknown sender.

2.3 Cybersecurity vs cybercrime

While the terms 'cybersecurity' and 'cybercrime' are interrelated and their interests often intersect, their meanings are not identical, and the scope of what constitutes 'cybersecurity' and 'cybercrime' varies from technical, legal and political perspectives.

The table below sheds some light on the scope of each regulatory domain:

Table 2: Defining Cybersecurity and Cybercrime

Cybersecurity	Cybercrime
Definition	
Cybersecurity is typically defined as the protection of confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT. The concept usually covers political (national interests and security), technical and administrative dimensions.	Cybercrime is defined as offences committed against computer data, computer data storage media, computer systems, service providers. The concept usually covers categories of offences such as illegal access, interfering with data and computer systems, fraud and forgery, illegal interception of data, illegal devices, child exploitation and intellectual property infringements.
Regulatory Focus	

[3] https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence
[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf
[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Cybersecurity	Cybercrime
Cybersecurity regulation focuses on protecting national infrastructure as well as the public and private sector against cyberattacks. A strong cybersecurity stance protects computer systems from unauthorized access or being otherwise damaged or made inaccessible. It aims to reduce the risk of cyberattacks and protects against the unauthorized exploitation of systems, networks and technologies through the use of technologies, processes and controls on technical, procedural and institutional levels. Cybersecurity focuses on the policy and procedure for securing and protecting systems and assets.	Cybercrime regulation focuses on outlining what the country considers cyber-dependent crimes and cyber-enabled crimes, providing the country with instruments to criminalize the offences and authorising investigation and prosecution of cybercrime offences. Cybercrime regulations provide focus on substantive law such as misuse of devices, procedural law such as preservation of data, and other provisions such as mutual legal assistance treaties and evidence collection. These are put in place in order to protect citizens by identifying those responsible for committing crimes, dismantling their operations, and bringing them as individuals/organized criminal groups to justice.
Incident Chronology	
Cybersecurity regulations typically work to prevent attacks *before* they occur. Security is a continuous cycle including incident response and revision of processes which happen *after* the detection of a breach.	Cybercrime regulations generally define and detect criminal activities in cyberspace *after* they occur, and provide powers to law enforcement to investigate the activities *after* they have occurred, to bring the offenders to justice.

A cybercrime strategy should, and must, work hand in glove with a cybersecurity strategy. In some cyber incidents, it may be unclear at the start whether it is a cybersecurity incident affecting personal, corporate or national infrastructure, or if it is a cybercrime incident where an actual crime is being committed, or if it is a combination of the two.

- In a cybercrime incident, a response would be required from law enforcement and the criminal justice system, for example the agency responsible for investigating cybercrime.
- In a cybersecurity incident, the relevant agency or entity responsible for cybersecurity would have to be deployed, e.g. a Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT).

The 2017 report by the European Union Agency for Cybersecurity (ENISA) "Tools and methodologies to support cooperation between CSIRTs and law enforcement"[6] also confirmed that CSIRTs and law enforcement often exchange information during incident handling/investigations, both formally and informally. Trust was quoted as a key success factor for effective cooperation. The report highlighted that, despite CSIRTs and law enforcement having different objectives and methods for collecting and processing information, there is an increased reciprocal understanding of needs between the two communities[7].

If a country has yet to develop and implement a cyber*security* strategy, the "NCSS Good Practice Guide" by ENISA is a useful document that can aid in that process[8].

[6] https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement
[7] https://www.enisa.europa.eu/publications/csirts-le-cooperation/at_download/fullReport
[8] https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

3. Factors that enable Cybercrime

A number of factors have contributed to the creation of a lucrative environment for cybercriminals and a vast population of potential victims. These include (but are not limited to):

3.1 Connectivity: more individuals online with low levels of digital security awareness

There is a rapid increase in the number of Internet users, and a directly related uptake in the use of mobile devices, e-commerce, electronic transactions and electronic communication. The generally poor awareness of cybersecurity and cyber hygiene, particularly amongst vulnerable users such as the elderly, **has led to a dramatic increase in the number of cybercrime victims.**

- A 2018 study by an American research university showed that the vast majority of home Internet users have poor cybersecurity awareness, e.g. were not aware of the difference between antivirus software and firewalls and had poor cyber hygiene, e.g. 67% of survey participants did not have either updated antivirus software or, in some cases, any antivirus even installed. Many users also freely share passwords and are quick to share private information over social networks[9].

3.2 Mobility: businesses online with staff working remotely on less secure networks

Greater mobility and wider network access have led to a sharp increase in the number of employees working remotely, including from home. As a direct result, more commercial and official communication and transactions are being conducted over less secure domestic or public computer systems and networks (e.g. people working from coffee shops). **This has increased the vulnerability of corporate networks and thereby increased the attack surface for cybercriminals.**

- A study released in August 2020 by INTERPOL revealed that phishing, online scams, fraud and other cyberthreats increased by as much as 59% following COVID-19[10].
- Amongst other threats, the World Economic Forum (WEF) reported in March 2020 that there was a need for businesses transitioning to work-from-home arrangements to ensure that there was a secure method for staff to connect to business-critical applications. There is also a need to ensure endpoint protection for all devices used by employees to access work resources online, such as multi-factor authentication[11].

3.3 Interconnectivity: cities and homes online, resulting in new forms of vulnerabilities

Smart Cities

The increased accessibility and miniaturisation of computer components has led to an acceleration in the deployment of Smart City networks and infrastructure. Examples of these networks of interconnected cities are the ASEAN Smart Cities Network[12] and India's Smart Cities Mission[13]. While the development of Smart Cities is a major goal for many economies, it also expands **potential attack surfaces available to cybercriminals who target vulnerable smart devices.**

[9] https://par.nsf.gov/servlets/purl/10083310
[10] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
[11] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/
[12] https://asean.org/asean/asean-smart-cities-network/
[13] http://smartcities.gov.in/content/innerpage/strategy.php

- In 2017, ransomware attacks such as WannaCry and NotPetya highlighted the threat these kinds of attacks can pose to interconnected networks, compromising a large number of devices[14].

Smart Homes

Smart Cities are not the only example of mass availability of Internet of Things (IoT) devices. The growing accessibility of smart home devices for consumers widens the number of potentially vulnerable devices. Many users of these devices fail to change default passwords or regularly update their software making them easy targets for attack. Common household items, such as door locks and refrigerators, have become Internet-capable devices providing an array of new options for cybercriminals to target.

- In 2019, Kaspersky noted that, in the first six months of the year, over 100 million attacks on smart devices were detected. This number is a dramatic increase from the previous year's 12 million detected attacks[15]. The report goes on to say that cybercriminals prefer residential devices over corporate devices[16] because they are usually easier targets.
- In 2020, Kaspersky honeypots – networks of virtual copies of various Internet-connected devices and applications – detected 426 million attacks on IoT devices coming from 742,000 unique IP addresses in the first six months of the year alone. This is a four-fold rise in the number of attacks, and 2.5 times the number of IPs compared to the same period last year.

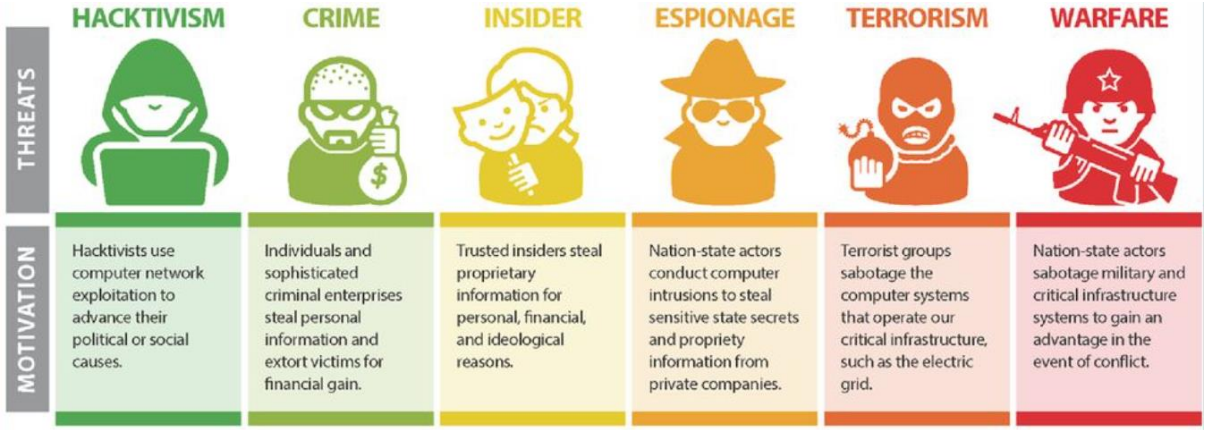
3.4 Sophistication: threat actors with evolving skills and tactics

Cybercrime is committed by threat actors with different motivations. They include:

- hacktivists who use the Internet as a means of protest
- criminals, such as:
    - opportunistic or curious beginners testing their skills
    - online child abusers
    - organized crime groups intent on making money
- nation-state sponsored advanced persistent threat (APT) groups who carry out espionage, raise funds or attack critical infrastructure.

Figure 1: Cyberthreat Spectrum

[14] https://www.wsj.com/articles/how-hackers-could-break-into-the-smart-city-11568776732
[15] https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019
[16] https://securelist.com/iot-a-malware-story/94451/



Source: unknown

Recent years have seen the evolution of cybercrime-as-a-service, where the 'corporatisation of cybercrime' put cybercriminal services within reach of anyone who is prepared to pay. Such transactions commonly take place on the DarkWeb, the hidden part of the Internet only accessible with special browsers. Cybercriminals take advantage of the anonymity of the DarkWeb's marketplaces and discussion forums to expand their skills and tools.

One example of cybercrime-as-a-service is Satan malware, which belongs to the Gen:Trojan.Heur2.FU ransomware family. Satan malware was made available to the public through a ransomware-as-a-service (RaaS) platform[17].

Large scale ransomware operations that cause widespread disruption and destruction to personal, corporate and national infrastructure are becoming increasingly commonplace:

- In 2020, fitness tracker company Garmin was attacked with the WastedLocker ransomware. The company reportedly paid $10 million (USD) ransom to the offenders to recover their systems and prevent user data from being publicly released[18] ;
- In October 2020, the US Cybersecurity & Infrastructure Security Agency (CISA) posted an alert on the increase in ransomware activity targeting the healthcare and public health sector[19].

3.5 Under-reporting: reluctance to report cybercrime offences

In many cases, companies and individuals who are victims of cybercrime do not report the incident to the authorities. **This failure to report crimes means there is a lack of data on how cybercriminals are operating and the technologies used to commit crimes.** Unfortunately, this is extremely widespread[20].

- Individual victims are often unaware of how or where to report cybercrime, believe that it is not worth reporting, or are ashamed that they have fallen victim to a scam[21]. In many cases, the incident did not result in loss of life or tangible property (such as personal data or information), and hence victims are unaware or unsure if they are victims of a crime and therefore do not report it to the authorities.

[17] https://www.zdnet.com/article/satan-ransomware-as-a-service-starts-trading-in-the-dark-web/
[18] https://www.wired.com/story/garmin-ransomware-hack-warning/
[19] https://us-cert.cisa.gov/ncas/alerts/aa20-302a
[20] https://www.zdnet.com/article/cyber-crime-under-reporting-of-attacks-gives-hackers-a-green-light-say-police/
[21] https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html

- Corporate victims are frequently reluctant to report cybercrime as making the news public is bad for business and could erode investor or market confidence in the company[22]. In many countries, this issue is being addressed by data protection regulations which mandate cyber incident reporting.
- In some cases, victims of cybercrime may find the reporting process to be onerous or unclear, thus deterring them from reporting the incident.

3.6 Legislation and jurisdiction: lack of criminalization of cybercrime and cross-jurisdictional complexity

Cybercrime frequently involves cross-border investigations as victims, offenders and infrastructure can be in different countries. This poses a challenge for investigators as they often discover that other countries may not have the same laws that criminalize the offence, or there are differing elements needed to prove the offence has taken place or that there are varying data retention periods for subscriber data. In some countries, there may even be a lack of legislation and therefore criminalization of cybercrime, which creates a situation where the country becomes a safe haven for cybercriminals.

It is also important for countries' legal frameworks to allow for adequate time for the collection, analysis and disclosure of digital evidence. Timelines that are too short may lead to critical evidence not being obtained, analysed properly or admitted in time, resulting in cybercriminals going unprosecuted.

Carrying out effective investigations across multiple jurisdictions also includes partnering with counterparts in another country in order to further an investigation. This may include conducting search and seizure of physical and/or digital evidence, or serve judicial authorisations such as warrants to private sector entities, e.g. telecommunication companies and Internet service providers.

These are just some of the difficulties involved in carrying out effective investigations across multiple jurisdictions in order to successfully prosecute cybercrime.

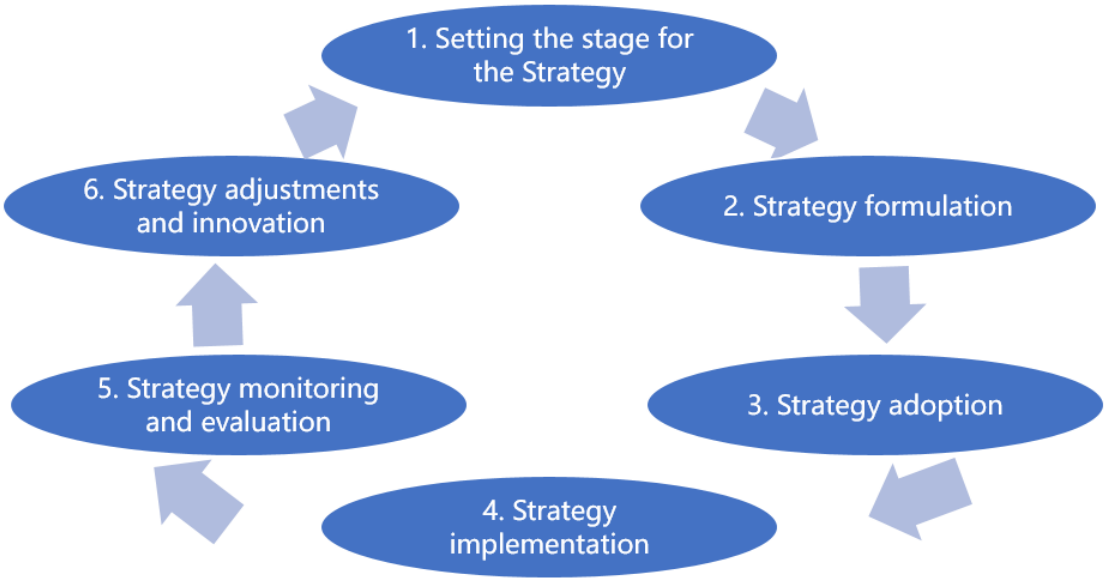
4. Methodology: Developing a Cybercrime Strategy

The initial task of developing a cybercrime strategy can seem overwhelming. Having a design process to follow will aid in crafting a strategy.

There are many models for policy design formulation, but generally the following processes are needed:

Figure 2: Strategy Life Cycle

[22] https://www.infosecurity-magazine.com/opinions/organizations-failing-report/



Source: TRPC, 2020

4.1 Setting the stage for the strategy

Before starting to develop a cybercrime strategy, it is important to understand why you are doing it.

Cybercrime is one of the fastest growing forms of transnational crime faced by INTERPOL's member countries. While rapid growth in ICT has enabled economic and social growth, an increasing reliance on the Internet has created more risks and vulnerabilities and opened up new possibilities for criminal activity.

The borderless nature of cybercrime means that law enforcement agencies face challenges in responding effectively due to the limits of cross-border investigation, legal challenges and diversity in capabilities across the globe.

A clear strategy is needed for a country to address these challenges and effectively protect its citizens from cybercrime.

There are many reasons for and benefits of developing a cybercrime strategy, as the following sections will discuss.

4.1.1 Cybercrime is economically destructive

In the June 2017 global NotPetya cyberattack, ransomware hit global logistics operators and their customers. Last minute rerouting, compensation, and keeping the global supply chain flowing cost Maersk up to $300 million (USD)[23]. The damage was not limited to their company, as their clients were also severely affected by the incident. Amongst others, medical supply company Merck lost $870 million (USD); FedEx's TNT Express lost $400 million (USD) and chocolate maker Cadbury lost $188 million (USD).

This domino effect of cybercrime was equally apparent when a large-scale DDoS attack using the Mirai botnet was launched against domain name provider Dyn in 2016, paralysing the business of many of the 178,000 customers who had their Internet domains hosted by the company[24]. These

[23] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[24] https://www.corero.com/blog/financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data/

incidents highlight the increasing sophistication and contagiousness of the new cybercrime methods which have evolved from earlier generations of cybercrime incidents such as Stuxnet, a computer virus which infected at least four oil and gas companies: Baker Hughes, ConocoPhillips, Marathon, and Chevron[25].

The World Economic Forum's Global Risk Report 2020 estimates the cost of cybercrime damages could reach $6 trillion (USD) in 2021[26].

A cybercrime strategy defines the necessary steps to take to institute good corporate data governance and personal cyber hygiene in order to limit economic impact.

4.1.2 Cybercrime enables other crimes

According to the United Nations Office on Drugs and Crime (UNODC) cybercrime incidents are frequently organized by crime networks operating online, which use ransom proceeds and other 'ill-gotten gains' to fund other forms of serious crime and terrorism[27].

A cybercrime strategy supports counter-terrorism and anti-money laundering (CT/AML) efforts, and curtails funding mechanisms for organized crime networks.

4.1.3 Cybercrime cripples government functions and can cost lives

Ransomware cyberattacks wreak havoc across all industries. In many cases, essential services are impacted, such as hospitals and healthcare agencies where lives can be lost as a result of computer systems being disabled. For example, in 2017, the WannaCry ransomware attack hit the United Kingdom's National Health Service (NHS), taking down medical systems, in some cases, while doctors were in the middle of critical operations such as heart surgery[28].

Similarly, in September 2020, a hospital in Düsseldorf, Germany suffered a ransomware attack. Due to the hospital's locked systems, a patient with a life-threatening condition had to be transferred to another hospital, where she died from the delay in treatment[29].

A cybercrime strategy must work in conjunction with a cybersecurity strategy to ensure that critical services are not disrupted.

4.1.4 Benefits of creating a strategy

Besides offering other benefits, a strategy:

- Informs everyone who can contribute positively and reap the benefits
- Gains a deeper understanding of a country's vulnerabilities
- Demonstrates progress in addressing the cybercrime challenge
- Provides for an established framework of prevention, detection, and response
- Raises awareness.

4.1.5 Requirements for a strategy

4.1.5.1 Establish a project authority

[25] https://isssource.com/stuxnet-hit-4-oil-companies/
[26] http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
[27] https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html
[28] https://www.dailymail.co.uk/news/article-4503420/It-s-life-death-NHS-patients-say-cyber-attack.html
[29] https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Development of a national cybercrime strategy requires cooperation from many different stakeholders. A common challenge in delivering a cybercrime strategy is securing and maintaining the commitment of relevant parties.

It is therefore important to identify a 'project authority' made up of a senior official, ideally a minister, and a project team with responsibility for developing, implementing and revising the cybercrime strategy.

The senior official owns the document and needs to ensure that:

- the project team receives the necessary cooperation from all key stakeholders;
- sufficient resources are available to implement the strategy.

As an example, the senior official could be the Minister of Home Affairs and the project team could consist of members of the national cybercrime unit. Alternatively, the project team could be a joint task force.

The project authority also sits on the steering committee (see section 4.2.1).

➔ Having the right leader and project team is essential for the successful delivery of the cybercrime strategy.

4.1.5.2 Obtain intragovernmental cooperation

For the development of a strategy to be effective, it requires intra-agency cooperation. This can prove difficult and requires good leadership, effective collaboration, and often compromise. Effective intra-agency cooperation is crucial for all stages of the project, such as the drafting and implementation of the cybercrime strategy.

The project authority should consult the relevant partner agencies to obtain their input and support.

Once agreement on the project concept is obtained, it is recommended that the project authority establish a mechanism to ensure intragovernmental cooperation. This cooperation mechanism may include periodic meetings of all relevant stakeholders, e.g. as part of a steering committee (see section 4.2.1).

➔ Ensure you have the buy-in of partner agencies before commencing the project.

4.1.5.3 Secure sufficient budget and resources

It is not unusual for government agencies to have financial and resource constraints. This can impact the ability to deliver the project and implement a national cybercrime strategy.

For the project to be successful, planning for and allocating dedicated and appropriate resources is vital. This includes money (i.e. dedicated budget) and people (i.e. dedicated project staff).

Similarly, an adequate allocation of human and financial resources is required for the implementation of the cybercrime strategy (see section 4.4.).

➔ Ensure you have sufficient resources before commencing the project.

4.1.5.4 *Set SMART goals*

The cybercrime strategy life cycle should follow the SMART Goals principles[30]: they should be Specific, Measurable, Achievable, Relevant and Time-Bound. The project should therefore start by establishing specific goals to be achieved within a specific timeframe, including measurable milestones and delivery dates.

Figure 3: SMART Goals

An example would be identifying the relevant stakeholders of the different stages of the cybercrime strategy life cycle within six weeks.

➔ Consider adopting this approach to clarify your ideas, focus your efforts, use your time and resources productively, and ultimately increase the chances of your project and cybercrime strategy succeeding.

4.2 Strategy formulation

This is the process where the cybercrime strategy is designed and drafted for the reasons and benefits set out in 4.1.

4.2.1 Designating the steering committee and identifying key stakeholders

Studies have shown that the success of public policies is often highly dependent on stakeholder engagement and management[31]. Strategies which fail to obtain stakeholder commitment, support, or ownership, often lack resources and attention and are not a priority.

As a first step, it is useful to create a steering committee comprising of the project authority and other relevant senior-level officials who should be selected based on their ability to provide strategic oversight and guidance at the different stages of the cybercrime strategy life cycle.

The steering committee should map out all stakeholders who need to be involved in the cybercrime strategy formulation. These consulting stakeholders ("the consultants") would typically come from government agencies and non-government entities.

Government Agencies:

- The National Cybercrime Unit so as to share experience and knowledge in investigating cybercrime;
- The lead agency for cybersecurity so as to share experience in cyber incident response and drafting of cyber*security* policies including strategies;
- Other Law Enforcement Agencies so as to provide assistance in understanding the regional issues and processes for investigating cybercrime, such as e-evidence collection;
- Relevant senior official(s) from applicable ministries, particularly those able to lend authority and support to the cybercrime strategy drafting or adoption. These may include officials from the Ministry of Home Affairs and the Ministry of Law or Justice, for example;
- Relevant prosecutorial and judicial officials to advise on the application of cyber-related laws in the country;
- Other relevant government officials and teams, such as those from bureaus responsible for investigating fraud, or officials from ICT Ministries, public safety and security, etc.

[30] https://www.achieveit.com/resources/blog/the-history-and-evolution-of-smart-goals
[31] http://www.oecd.org/gov/regulatory-policy/BPPs-for-Public-Consultation.docx

Non-Government Entities:

- Academics/think tanks capable of providing knowledge of current issues, while also offering research and drafting skills;
- Technology/industry bodies best placed to identify the most significant threats facing businesses;
- Civil society groups to help raise public awareness;
- Regional and international bodies to share perspectives on regional cybercrime threats.

Selecting the right consultants will cover the full gamut of stakeholders' needs and provide a better foundation for the drafting of the cybercrime strategy. Any stakeholders who were not consulted in the early stages but brought on board at a later date may cause disruption and even undermine all previous efforts.

Following the identification of the consultants, a smaller group of the best suited individuals for the drafting activity ("the drafters") is then selected for the subsequent production of the strategy (see section 4.2.3 Production).

4.2.2 Stocktaking, assessment and analysis

It is crucial for a country to take stock of their available processes, resources and skills to combat cybercrime. This exercise will also provide valuable insights into areas where there are deficiencies. As a result of this, a country will have a clearer view of their current cybercrime landscape and can start to work towards building their desired future in terms of strengthening their overall capability to combat cybercrime.

The stocktaking audit should take into account the following categories:

4.2.2.1 People and equipment

This audit assesses the human resources available or working in a cybercrime-related function, e.g. cybercrime and digital forensics personnel, cybersecurity personnel including CERTs.

Some examples of agencies who could be listed here include:

- National police agency – departments and units
- National cybersecurity agency or department (if any)
    - National Computer Security Incident Response Team (CSIRT) and/or CERT
- National, regional and state/province level justice or law ministry
    - dedicated cybercrime judges
    - dedicated cybercrime prosecutors
    - investigations branch
- Central Authority for managing Mutual Legal Assistance Treaties (MLATs)
- National security or intelligence agency
- Other national agencies responsible for cyber-enabled crime (e.g. fraud, exploitation, etc.)
- Other state or province-level police services with active cybercrime investigation units.

Each of these agencies should provide a report on the following:

- A summary of their agency and relevant unit's organisational structure and mandate
- An explanation of the types of cybercrime that the agency covers
- The legal framework they operate in
- Current anti-cybercrime initiatives in place by any of the agencies.

Also consider the technological capabilities of the various agencies – do they have the right equipment and related training to do the job?

4.2.2.2 Process: Assessing the legislative and regulatory environment

This takes stock of existing legislative and regulatory mechanisms that deal with cybercrime in the country. It includes all relevant legislation, international cooperation agreements, internal operating procedures and standards, local customs and practices etc.

Process issues may fall into the following categories:

- **Substantive legislation** such as laws covering personal data protection or data privacy; laws criminalising offences such as hacking and data theft; laws criminalising the sale of tools or services for hacking; laws against online harassment; and laws outlining requirements for protecting critical infrastructure.
- **Procedural legislation** such as laws on the collection and use of electronic evidence; rules on search and seizure of electronic evidence; rules on electronic surveillance.
- **International cooperation agreements** such as MLATs, accession to the Budapest Convention[32], active use of INTERPOL membership to access international cooperation systems.

The consultants may review existing legislation and identify gaps in the country's current legal framework. In some cases, there may also be a need to merge a number of different laws. This could also include updating laws to adequately criminalize cybercrime and updating regulations which legalize and provide for the search, seizure and admissibility of electronic evidence in criminal investigations. In addition to cybercrime legislation, the investigatory power of law enforcement agencies, jurisdictional issues, data protection, privacy, and commercial law in relation to confiscation of cybercrime proceeds may need to be reviewed.

4.2.2.3 Self-assessment and analysis

Once the stocktaking audit has been completed, an assessment should be conducted to identify vulnerabilities and areas for improvement. There are several toolkits available for conducting national assessments and measuring the cyber capability of a country.

A periodic global cyber assessment by country is conducted by the International Telecommunication Union (ITU), which monitors and compares countries' cybersecurity commitments by examining five pillars: legal, technical, organisational, capacity building and cooperation. It also factors in results from other existing assessment tools such as the Capability Maturity Model (CMM) and the Potomac Institute's Cyber Readiness Index. The resulting product is referred to as the Global Cybersecurity Index (GCI)[33].

An in-depth self-assessment tool is the World Bank's 2017 Combatting Cybercrime Assessment Tool and Toolkit. This resource[34] is comprised of the Assessment Tool[35], which is an automated excel file that enables a user to determine gaps in their current capacity to combat cybercrime and highlight areas towards which to direct resources. An accompanying guidebook (the Toolkit[36]) provides a contextual background to the Assessment Tool. The first use of the Assessment Tool provides a baseline which can then be monitored periodically. The Assessment Tool and Toolkit should be used in tandem.

The ITU's Global Security Index is generally published once every year but countries can conduct a self-assessment using the World Bank Assessment Tool and Toolkit at their convenience.

---

[32] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[33] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[34] https://www.combattingcybercrime.org/
[35] https://www.combattingcybercrime.org/#assessment
[36] https://www.combattingcybercrime.org/#toolkit

The results of the assessment that the country performs will highlight vulnerabilities and areas for improvement. These should be considered as focus areas for the strategy, as discussed in the next section.

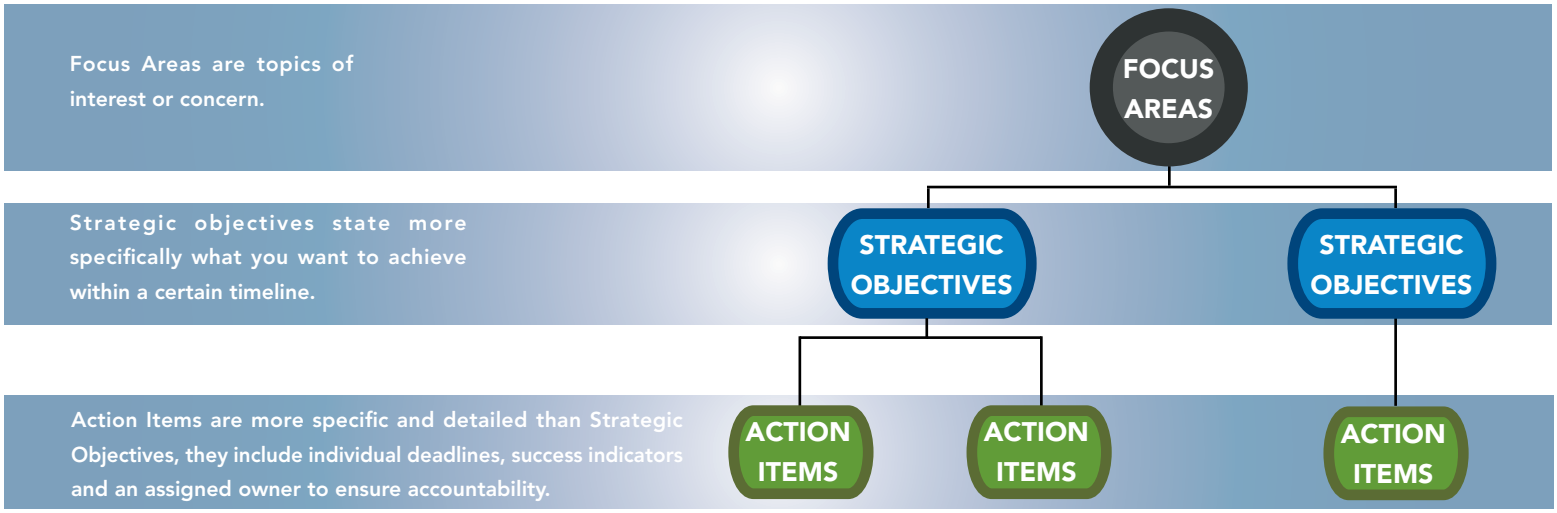
Depending on the assessment tool you use and its output, it may be beneficial to consider structuring the results using tried-and-tested analysis methods such as:

- SWOT – strengths, weaknesses, opportunities and threats
- PESTLE – political, economic, social, technological, legal and environmental.

The method selected should allow policymakers to determine which of the gaps identified from the self-assessment need to be prioritized for immediate, medium term and long term action.

4.2.2.4 *Focus Areas, Strategic Objectives and Action Items*

Figure 4: Focus Areas, Strategic Objectives and Action Items



A country will identify the Focus Areas it wishes to address, such as the legal framework, from its self-assessment and analysis (section 4.2.2.3). Strategic Objectives are then defined for the Focus Area, e.g. 'develop a more effective legal framework to investigate and prosecute cybercrime'. This will prompt one or more Action Items that are to be completed by "action owners", e.g. update existing cybercrime laws and draft new ones.

Focus Areas – those areas the country seeks to improve - are the cornerstone of the strategy which the country defines based on the results of the self-assessment and analysis. This is the first step in creating the structure to ensure the country will be in a stronger position to combat cybercrime.

Focus Areas are the broad themes of the strategy and have a longer lifespan than the Strategic Objectives and Action Items.

Strategic Objectives are clearly defined statements of outcomes that a country aspires to achieve within a defined timeframe.

Action Items are identified by the project authority and relevant stakeholders (section 4.2.1, "consultants") based on their suitability to help attain the Strategic Objectives. Action Items should follow the SMART model (section 4.1.5) and should try to answer these questions:

- How can the Strategic Objective be achieved?

- Are there existing programmes or mechanisms in place that address the Strategic Objective?
- How can the existing programmes or mechanisms be improved?
- What new programmes or mechanisms need to be created or developed?
- How will these be implemented?
- What is the timeline?
- How will their success be measured (success indicators)?

Once the Focus Areas, Strategic Objectives and Action Items have been clearly established, they can be summarized in a simple reference table, such as the one below:

Table 3: Example of Summary Table for Focus Areas, Strategic Objectives and Action Items

Focus Areas	Strategic Objectives	Action Items
Legal Framework	Develop a more effective legal framework to investigate and prosecute cybercrime	• Draft and implement relevant laws on cybercrime within 18 months (implementing agency: Ministry of Law) • Secure accession to the Budapest Convention on Cybercrime within two years (implementing agency: Joint task force between Ministry of Law and Ministry of Foreign Affairs)
Capacity Building	Ensure capacity building for public servants, particularly law enforcement, prosecutorial and judicial authorities	• Develop and establish a cybercrime curriculum and training for law enforcement authorities, to start within 12 months (implementing agency: Ministry of Home Affairs/ Ministry of Public Security or similar) • Develop and establish training on digital evidence fundamentals for judges and public prosecutors, to start within 12 months (implementing agency: Attorney General's Office, Ministry of Law/Ministry of Justice)
Partnerships	Promote national and international information sharing arrangements and alliances	• Create public-private sharing agreements on cyber intelligence within eight months (implementing agency: Cybercrime Department of the Police Force) • Put in place a cyberthreat alert system within nine months between public and private sector, prioritising critical industries (implementing agency: Joint task force between Cybercrime Department and Ministry of Industry and Trade, working with other relevant ministries)

4.2.3 Production

The production of the cybercrime strategy is the stage of the strategy life cycle likely to take the most time. To aid with drafting efforts, this Guidebook provides a template to assist countries (Chapter 5).

4.2.3.1 Stakeholder consultations

An iterative process should be undertaken with the Focus Areas being put forward for discussion with the stakeholders ("consultants"). This provides contributors to the strategy with the opportunity to provide input on how progress can be made in the Focus Areas, thus shaping the Strategic Objectives (see section 5.4).

4.2.3.2 The first draft of the cybercrime strategy

This is the point at which the previously identified group of drafters (section 4.2.1) create a first draft of the cybercrime strategy bearing in mind the reasons and benefits outlined in section 4.1 and the results of the stocktaking exercise described in section 4.2.2.

It is usual practice for a draft strategy to undergo a number of stages of writing, consultation, feedback, review and amendment. The more thoroughly this is done, the more likely that the final strategy will achieve stakeholder consensus.

The drafters can refer to the Cybercrime Strategy Template (chapter 5) for a proposed structure of the document.

4.3 Strategy adoption

Once the strategy formulation process is completed, a finalized draft of the cybercrime strategy is ready to be presented formally for adoption and implementation.

This process will differ from country to country. Some countries will require the strategy to be debated in a national assembly, parliament, or some other public policy forum before being presented for endorsement, e.g. passed in Parliament/National Congress/Assembly, or submitted to the Head of Government/State for approval.

4.4 Strategy implementation

In order for the cybercrime strategy to succeed, there must be a structured approach to implementation. The implementation will differ from one country to another but will generally involve the following steps:

- determining the specifics of how the Strategic Objectives will be met (section 4.2.2.4)
- developing separate implementation plans per Action Item
- allocating adequate human and financial resources.

The project authority together with the consultants needs to develop Action Items and implementation plans in support of the Strategic Objectives and identify specific officials or units as owners ("action owners"). The action owners should be representatives from agencies/units that are the most relevant to the action assigned to them and have the best capability for successfully implementing it.
These officials or units would then be responsible and accountable for the implementation of the specific plan assigned to them. As the implementation plans are intended to be executed at a working level, they should be defined so as to be clearly understood by the implementing agencies (action owners).
The project authority may need to coordinate the implementation of the various plans.

The steering committee may need to assist in securing adequate resources for the implementation of the various plans. This will ensure that all efforts up to that point were not in vain.

It is recommended that the implementation plans include specific metrics and success indicators to monitor the progress of each of the Action Items.

4.5 Strategy monitoring and evaluation

In line with the SMART goals (section 4.1.5.4) of the cybercrime strategy, the project authority and the consultants should also plan for the strategy to be monitored and evaluated at regular intervals, to keep up the momentum of progress. Failure to continuously monitor the implementation efforts may jeopardize not only individual Action Items but the entire project.

Continued engagement with and reporting by the action owners on previously defined metrics will help to keep the implementation of the cybercrime strategy on track. Monitoring should focus on details about the progress of implementing activities, availability of resources as well as issues and risks that may be impeding the implementation of the plan. The project authority should be made

aware of any delays in good time so that mitigation plans can be put in place. Conversely, the project authority should also be notified of achievements so that they can be recognized.

4.6 Strategy adjustments and innovation

Just as the initial cybercrime strategy drafting process was an iterative process, the finalized cybercrime strategy should equally be reviewed on a periodic basis to keep pace with technology, new attack vectors and the ever-changing needs of the country.

Example: Evolution of New Zealand's Cybersecurity and Cybercrime Strategy

The example of how New Zealand's cybercrime strategy progressed illustrates the process that many countries have embarked upon in order to adopt a guiding framework which remains relevant in view of evolving economic and societal trends. It also illustrates that a country's Cybercrime Strategy needs to be aligned with and fit into a broader scheme of national policies, all of which are subject to continuous revision cycles.

New Zealand's 2011 Cyber Security Strategy outlined the government's response to the growing cyberthreat by defining priority areas, initiatives and allocating appropriate resources.

In 2015, a refreshed (second) Cyber Security Strategy with an accompanying Action Plan was published replacing the 2011 Cyber Security Strategy; a **National Plan to Address Cybercrime**[37] (akin to a Cybercrime Strategy) was also released to ensure an appropriate cybercrime response by defining the following priority areas:

- build capability to address cybercrime
- adapt the country's policy and legislative settings to the digital age
- enhance operational response to cybercrime
- use New Zealand's international connections to combat cybercrime.

In 2019, New Zealand published its 3rd Cyber Security Strategy[38] which outlines updated priority areas on cybersecurity and updated key focus areas on cybercrime.

Figure 5: New Zealand's National Action Plan to Address Cybercrime

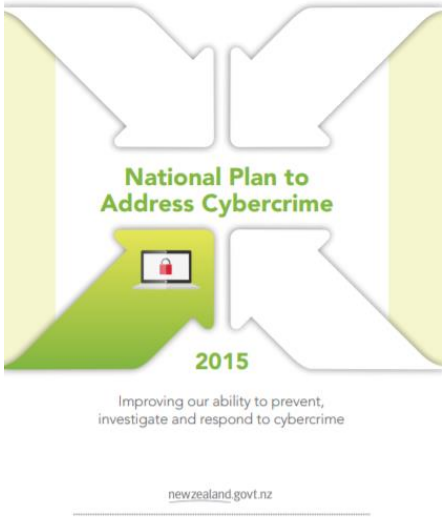


Figure 6: Evolution of New Zealand's Cybersecurity and Cybercrime Strategy

[37] https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf
[38] https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

5. The Budapest Convention

While the aim of a country's cybercrime strategy is to strengthen its overall ability to combat cybercrime domestically, particular consideration should also be given to aligning it with international standards and practices. A country developing or updating a Strategy should aim to have its legal frame and other strategic objectives correspond with the requirements for accession to the most comprehensive and coherent international agreement on cybercrime and electronic evidence, the Convention on Cybercrime of the Council of Europe, commonly known as the Budapest Convention.

5.1 About the Convention

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with offences against and by means of computer systems and data, such as illegal access, illegal interception, data and system interference, computer-related fraud, child sexual exploitation material or other violations of network security. It also contains a series of powers and procedures for criminal investigations and the securing of electronic evidence in relation to any crime where evidence is on a computer system, such as expedited preservation, searching computer networks or interception.

Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[39] The Convention aims principally at:

(1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;

(2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; and

(3) setting up a fast and effective regime of international co-operation.[40]

The Convention was opened for signature in Budapest, Hungary, in November 2001. In 2003, it was complemented by a Protocol on Xenophobia and Racism committed via a computer system. A new, 2nd Protocol is expected to be available soon to provide for enhanced cooperation and disclosure of electronic evidence, including direct cooperation with service providers and cooperation in emergency situations.

5.2 Benefits of the Convention

Any country may make use of the Budapest Convention as a guideline, checklist or model law. However, becoming a Party to this treaty entails additional advantages:

- The Convention provides a legal framework for international cooperation on cybercrime and electronic evidence. Chapter III of the treaty makes general and specific provisions for cooperation among Parties "to the widest extent possible" not only with respect to

[39] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[40] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680occe5b

cybercrime (offences against and by means of computers) but with respect to any crime involving electronic evidence.

- Parties are members of the Cybercrime Convention Committee (T-CY). Parties share information and experience, assess implementation of the Convention, or interpret the Convention through Guidance Notes.
- The T-CY may also prepare additional Protocols to this treaty. Thus, even if a State did not participate in the negotiation of the original treaty, a new Party is able to participate in the negotiation of future instruments and the further evolution of the Budapest Convention.
- Parties to the Convention engage with each other in trusted and efficient cooperation. Indications are that private sector entities as well are more likely to cooperate with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime and electronic evidence in place, including the safeguards of Article 15.
- States requesting accession or having acceded may become priority countries for capacity building programmes. Such technical assistance is intended to facilitate full implementation of the Convention and enhance the ability to cooperate internationally.

5.3 Accession to the Convention

Under Article 37 of the Convention, any State can join the treaty and become a Party to the treaty by "accession" if the State is prepared to implement the provisions set out in the Convention. The accession procedure is as follows:

1.Once a (draft) law is available that indicates that a State has already implemented or is likely to implement the provisions of the Budapest Convention in its domestic law, the Minister of Foreign Affairs (or another authorised representative) sends a letter to the Secretary General of the Council of Europe stating the interest of his or her State in acceding to the Budapest Convention.

2. The Council of Europe then consults the other Parties and, once an agreement has been reached among the current Parties to the Convention, the State is invited to accede.

3. The authorities of that State complete their internal procedures similar to the ratification of any international treaty before depositing the instrument of accession at the Council of Europe.[41]

6. Cybercrime Strategy Template

This chapter provides a template to guide drafters who are in the initial stages of creating their own cybercrime strategy. It covers the points discussed in previous chapters and provides some additional guidance on structure and content.

[41] https://rm.coe.int/cyber-buda-benefits-june2020a-en/1680a6be38

This template includes recommended elements that are commonly observed in cybercrime strategies, but we recommend that drafters take their local context and regulatory framework into consideration.

There are four main components to a cybercrime strategy:

- Introduction
- Current cybercrime landscape - assessment and analysis
- Vision
- Focus Areas, Strategic Objectives and Action Items.

6.1 Introduction

This first section is an introduction to the country's cybercrime strategy. It should allow readers to understand the nature of cybercrime in the country. It may include sub-sections such as those described below.

6.1.1 Foreword

This could be a message from someone who endorses and drives the strategy such as the competent minister or another senior political official. This introduction should show why the strategy is important and demonstrate that it has support and 'buy-in' from senior leaders and that there will be an expectation of delivery. The project authority should also be introduced.

6.1.2 Purpose of the document

This part describes what the strategy will be used for and how it will help the country.

6.1.3 Background on why the strategy is necessary

This could include a short overview of how strategies for addressing cybercrime have evolved in the country, and provide the justification for the cybercrime strategy (see section 4.1).

Some statistics could be cited (if available), such as the cybercrime incident figures, the number of local Internet and/or mobile device users, the financial impact on the country and on individual victims. These figures will put the current cybercrime situation in perspective and statistics on the uptake of new technologies may provide valuable insight into potential future cybercrime attack vectors, e.g. vulnerable IoT devices.

Where countries do not have comprehensive data on cybercrime, they could use global figures as an indicator.

6.2 Current cybercrime landscape

6.2.1 Cyber-related definitions

This section provides a clear definition of what the government considers to be cyber-dependent crime, cyber-enabled crime and cybersecurity (sections 2.2 and 2.3). It could also refer to the different types of cybercriminals or threat actors (section 3.4), and quote statistics on cybercrime that may be relevant.

6.2.2 Cybercrime statistics within the country

This section will break down the high-level statistics from section 5.1.3 by relevant metrics, such as crime type, region, demographic etc. This will help highlight the specific and most prevalent cybercrimes occurring in the country.

Some examples of figures and trends which could be reported here include:

- the number of cyber-dependent crime attacks by type, e.g. ransomware attacks in a given period;
- the number of cyber-enabled crimes reported in a given period;
- the main types of cybercrime (website defacement, ransomware, phishing, child abuse material, online harassment etc.);
- rise in different types of cybercrime as a percentage and actual figures over a given period, e.g. year-on-year.

The Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence[42] lays out the agenda for compiling criminal justice statistics with key steps for data collection, analysis and cooperation among multiple stakeholders.

6.2.3 Existing cybercrime authorities

This section identifies all relevant national and state/ provincial level agencies and authorities responsible for investigating, combating and prosecuting cybercrime. It elaborates on their roles within the criminal justice system and their mandates (section 4.2.2.1).

The objective is to provide a clear understanding of the responsibility of each authority, their jurisdiction, investigative areas, initiatives and the scope of cyber-related crimes that they tackle.

6.2.4 Existing legislation

This section of the cybercrime strategy outlines cybercrime legislation which has already been enacted (section 4.2.2.2).

This may include:

- cybersecurity law/act
- computer crimes act
- substantive criminal laws
- procedural laws, i.e. provision of basic subscriber information, traffic data, content data
- international cooperation laws and/or agreements, such as MLATs
- data protection laws, including data retention regulation for data custodians/data processors
- any other act which gives authority to the prevention, investigation or prosecution of cybercrime.

6.2.5 Self-assessment and analysis summary

This section should include the results from the self-assessment and analysis process described in Section 4.2.2.3 which maps out a country's capacity to combat cybercrime, as well as any gaps which need to be addressed. This assessment will serve as the foundation for the identification of the strategy's Focus Areas, Strategic Objectives and Action Items (section 5.4).

6.3 Vision

This section lays down a clear government vision for governing cybercrime. It usually takes the form of a brief summary of the government's desired strategic success. Some examples include:

[42] https://www.interpol.int/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf

- "The vision of the NCAP is to ensure a safe and secure online environment for Singapore. We will achieve this by effectively deterring, detecting and disrupting cybercriminal activities." - Singapore's National Cybercrime Action Plan (NCAP)[43];
- "Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience." - United Kingdom's Home Office's Cyber Crime Strategy[44];
- "The RCMP Cybercrime Strategy's vision is to reduce the threat, impact and victimisation of cybercrime in Canada through law enforcement action." - Royal Canadian Mounted Police (RCMP) Cybercrime Strategy[45].

This vision should ideally set a clear whole-of-government and whole-of-society approach for combating cybercrime, especially as it is a shared responsibility where government, citizens, businesses and civil society work together to deter, detect and disrupt cybercrime. The clearer the vision, the easier it will be for leaders and key stakeholders to ensure a comprehensive, consistent and coherent approach.

6.4 Focus Areas, Strategic Objectives and Action Items

This section of the document will form the largest part of the cybercrime strategy. It follows on from the self-assessment and analysis (section 4.2.2.3). Based on the results, it will identify the Focus Areas which the government considers crucial for the effective combating of cybercrime. These should then be translated into Strategic Objectives and Action Items (section 4.2.2.4), which can then be assigned to the relevant agencies (action owners) and tracked (section 4.5).

6.4.1 Focus Areas

As described above, the Focus Areas will be derived from the self-assessment and analysis (section 4.2.2.3). The Focus Areas should then be detailed and clear definitions should be provided together with a justification for their selection.

6.4.2 Strategic Objectives

Several Strategic Objectives can align to one Focus Area. They state more specifically what should be achieved within a certain timeline.

6.4.3 Action Items

Action Items are more specific and detailed than the Strategic Objective; they include individual deadlines, success indicators and an assigned owner to ensure accountability. More than one Action Item can contribute to one Strategic Objective.

6.4.4 Examples of Strategic Objectives and corresponding Action Items

The following section provides examples for countries looking to develop their cybercrime strategy's Strategic Objectives. See also section 4.2.2.4, particularly table 3.

6.4.4.1 Strategic Objective 1: Develop a more effective legal framework to investigate and prosecute cybercrime

[43] https://www.mha.gov.sg/docs/default-source/press-releases/ncap-document.pdf
[44] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf
[45] https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

The legal framework of many countries does not effectively criminalize cybercrime. In such circumstances, the number of cybercrime cases will continue to rise while legislation remains one step behind.

A Strategic Objective could be to update the legal framework and leverage international frameworks or instruments to address current challenges that are experienced in the investigation, enforcement and adjudication of cybercrime.

Action Items with timelines and implementing agency

- Draft and deliver a law on cybercrime within *a determined period* (potential implementing agencies: Ministry of Law or Department of Home Affairs or Attorney General's Office);
- Ensure accession to the Budapest Convention on Cybercrime within two years (potential implementing agencies: joint task force between Ministry of Law and Ministry of Foreign Affairs).

6.4.4.2 Strategic Objective 2: Capacity-building for criminal justice authorities

Cybercrime offences have increased in volume and complexity, which creates additional demand for the continuous training of criminal justice authorities (e.g. police, prosecutors and judges) dealing with these crimes. At the same time, digital evidence plays an increasingly important role in many types of criminal cases. Maintaining the integrity of digital evidence from collection to presentation in court is often a key component of successful prosecutions.

As digital devices and electronic evidence are components of almost all types of crime, even 'non-specialized' law enforcement officers require a basic understanding of digital evidence as well as the proper way to seize it.

Prosecutors and judges rely on the lawful collection of accurate and reliable evidence for presentation and admission in court. Convictions also often depend on prosecutors and judges sufficiently understanding digital evidence.

A Strategic Objective could therefore be to build relevant capacity among the nation's criminal justice authorities responsible for the prevention, investigation, prosecution and adjudication of cybercrime.

Boosting the investigative capacity of law enforcement officials will make them more effective at combating cybercrime and may simplify collaboration with other government agencies and private industries.

Increasing the capacity of prosecutors and judges will help them correctly interpret and introduce/admit electronic evidence in court.

Action Items with timelines and implementing agency

- Establish and continuously review a cybercrime training curriculum for law enforcement within six months (suggested implementing agency: Ministry of Home Affairs/Ministry of Public Security or similar);
- Conduct a minimum of five cybercrime investigation trainings per year for law enforcement officers, to start after implementation of the training curriculum (suggested implementing agency: Ministry of Home Affairs/Ministry of Public Security or similar);
- Establish and conduct at least one training on the fundamentals of digital evidence for all judges and public prosecutors handling cybercrime cases, to start within eight months (suggested implementing agency: Ministry of Law, Attorney General's Office).

6.4.4.3 Strategic Objective 3: Fostering partnerships to combat cybercrime

While cybercrime and cybersecurity personnel have the responsibility to work towards safer cyberspace, they cannot succeed alone. The assistance of other national agencies, other countries and other sectors can be vital for enhancing their knowledge and capabilities.

Intragovernmental collaboration

Some agencies tend to work in silos and the same may be true when it comes to information sharing between national agencies. Knowledge, intelligence and resources are often spread out over several agencies with little awareness or poor coordination of information, initiatives, investigations and capabilities between them.

A Strategic Objective could be to promote inter-agency sharing of information and resources which can lead to a significantly more effective approach to combating cybercrime.

Intergovernmental collaboration

Offenders communicate and operate across borders without any restriction putting them at an advantage over the authorities tasked with bringing them to justice.

A Strategic Objective for a country could be to expand its use of international networks, such as law enforcement and prosecution officials. These networks often exchange information on a reciprocal basis via mechanisms of varying formality, rendering their work more effective.

National law enforcement agencies have a variety of cooperation mechanisms at their disposal, both on a formal - MLAT for example - and more informal basis in order to expedite the transfer of information between agencies. Established 24/7 networks, such as the INTERPOL I-24/7, G8 24/7 High Tech Crime Network and the 24/7 network of contacts of parties to the Budapest Convention on Cybercrime have been developed to receive urgent requests for digital evidence and facilitate international cooperation.

There are also dedicated mechanisms for cybercrime prosecutors, such as the International Association of Prosecutors' Global Prosecutors E-Crime Network (GPEN).

Public-Private Partnerships

Preventing and investigating complex cyber incidents requires significant technical skills and resources, which may be more readily available in private-sector organisations than in law enforcement.

Stronger multi-level collaboration between the public and private sector will go a long way in enhancing a country's cybercrime response, while a better informed public will reduce the number of potential victims.

A Strategic Objective could be to form public-private partnerships across different sectors for the benefit of both cybercrime prevention and criminal investigation. These partnerships with entities such as telecommunications providers, financial services and cybersecurity companies may focus on different aspects such as raising awareness, technical training, analysis and investigation assistance through information and intelligence sharing. Topics could include information on cyberthreats, trends, vulnerabilities and how to tackle particular incidents.

An additional Strategic Objective could be to raise awareness amongst the general public about common cyberthreats. Public-private initiatives like the United Kingdom's Get Safe Online programme[46] provide practical advice to the public on how they can protect themselves, their

[46] https://www.getsafeonline.org

computers and mobile devices and businesses against fraud, identity theft, viruses and many other problems encountered online.

Partnerships with multinational organisations

Partnerships with the right organisations can have a direct impact on a country's ability to combat cybercrime as they provide opportunities for information exchange and intelligence sharing which may help in investigations and other areas. They can also have an indirect impact through networking and resource exchange in the form of equipment donations or temporary secondments of personnel to certain partner organisations. International and regional partners can additionally provide avenues for capacity building and sharing of best practices, an example being this Guidebook.

A Strategic Objective could be to establish and maintain relevant partnerships at the global and regional level.

At the global level, organisations such as INTERPOL, UNODC, ITU, the World Bank and Information Sharing and Analysis Centers (ISACs) can be valuable partners.

At the regional level, partnerships with organisations such as ASEAN or ASEANAPOL, Europol, the African Union, the Organization of American States (OAS), the Economic Cooperation Organization (ECO), Caribbean Community (CARICOM) and the Implementing Agency for Crime and Security (IMPACS), to name but a few, can be highly beneficial.

Action Items with timelines and implementing agency

- Create a cybercrime "clearing house", a central body that deconflicts the work of the various national stakeholders engaged in the investigation and prosecution of cybercrime incidents. This should also include a single crime reporting channel to prevent duplication of investigations. Implementation within 12 months, driven by the relevant ministries;
- Encourage and optimize the use of relevant 24/7 networks, effective immediately. Implementing agencies are those responsible for the operation of the criminal justice system, e.g. Ministry of Home Affairs/Ministry of Public Security, Department of Justice;
- Facilitate the concluding of formal intelligence sharing agreements within six months between public and relevant private sector entities to aid in identifying cyberthreats against critical industries, i.e. energy, water, healthcare, communication, finance, transportation etc. Potential implementer: national cybercrime unit;
- Promote good cyber hygiene through awareness campaigns such as the annual Safer Internet Day[47] in February. Implementation within six months; potential implementers: national cybersecurity agency and national cybercrime unit;
- Fully explore and leverage information and intelligence available from or through organisations like INTERPOL, e.g. the INTERPOL Global Cybercrime Expert Group (IGCEG) and Cyber Activity Reports (CAR) with immediate effect. Implementing agency: national cybercrime unit or relevant ministry.

6.4.5 Appendices

5.4.5.1 Glossary

It may be useful for the cybercrime strategy to also include a glossary which defines key terms, abbreviations and acronyms.

[47] https://www.saferinternetday.org/

5.4.5.2 References

Links to references which may provide further guidance.

Appendix A: National cybercrime and cybersecurity strategies and regulations

This appendix provides a list of publicly available resources and references to which countries may wish to refer when formulating their own cybercrime strategy. Some countries have chosen not to publicize their cybercrime strategy, which is an option if there is concern over public disclosure.

In many cases, a cybercrime strategy is designed to complement the cybersecurity strategy. In other cases, a cybercrime strategy already forms part of the cybersecurity strategy.

Australia

- Cyber Security Strategy (2020)
  https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf

Canada

- National Cyber Security Strategy (2018)
  https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
- Royal Canadian Mounted Police Cybercrime Strategy (2014)
  http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

Europe/European Union

- Budapest Convention and related standards (2001)
  https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
- European Union Agency for Cybersecurity (ENISA) - NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies (2016)
  https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

New Zealand

- National Plan to Address Cybercrime (2015)
  https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf
- Cyber Security Strategy (2019)
  https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

Singapore

- Singapore Cybersecurity Strategy (2016)
  https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

United Kingdom

- National Cyber Security Strategy 2016-2021
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- Cyber Crime Strategy (2010)
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

United States of America (2018)

- National Cyber Strategy of the United States of America
  https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

International Telecommunications Union (ITU)

- Guide to Developing a National Cyber Security Strategy (2018)
  https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

INTERPOL

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Our role is to assist law enforcement agencies in our 194 member countries to combat all forms of transnational crime. We work to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Our services include targeted training, expert investigative support, specialized databases and secure police communications channels.

OUR VISION: "CONNECTING POLICE FOR A SAFER WORLD"

Our vision is that of a world where each and every law enforcement professional will be able through INTERPOL to securely communicate, share and access vital police information whenever and wherever needed, ensuring the safety of the world's citizens. We constantly provide and promote innovative and cutting-edge solutions to global challenges in policing and security.