CREST

CMAGE
Cyber Security Maturity Assessment Global Ecosystem

Good Practice Guide

Developing and Implementing Cybercrime Prevention into the CREST Cyber Security Ecosystem for Asia and Africa

June 2022

Government

Developing and Implementing Cybercrime Prevention

Contents

Foreword

In 2020, UK-headquartered CREST International, a not-for-profit accreditation and certification body for the technical security industry, received a grant from the Bill & Melinda Gates Foundation. The purpose of the grant is to fund research, better understand and help increase cyber security capacity in developing countries in Asia and Africa.

The foundation specified its objective as follows: "*to build trusted cybersecurity expertise in individuals and organizations in low-income countries and enable local markets to address the growing cyber-risk in digital financial services.*" Bill & Melinda Gates Foundation, 2021.

To determine the cybersecurity eco system status, CREST developed and utilised its evaluation model, the Cybersecurity Maturity Assessment of the Global Ecosystem (CMAGE). Part of the evaluation considered the country's status in cybercrime law enforcement. It highlighted the need for a robust, resourceful criminal justice response.

It also highlights the requirement to enhance law enforcement capabilities in tackling cybercrime, and the necessity to prevent entry into, and escalation of, cybercrime.

The evaluation also highlighted the absence of Cyber Security Prevent Programmes and the lack of guidance available on how they should be established and operated.

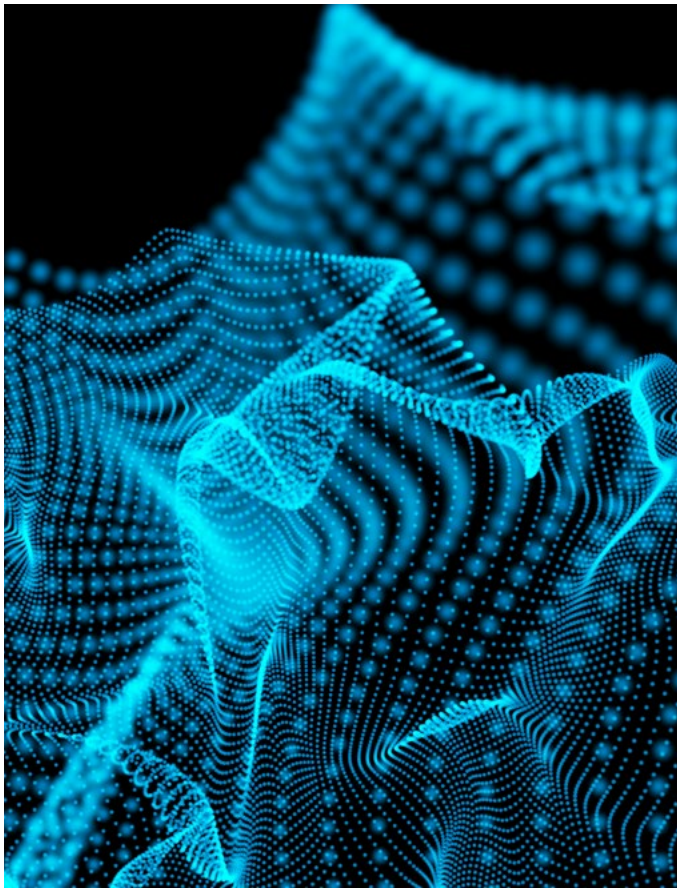
This report outlines how to design, develop and deliver a Cybercrime Prevention programme.

From a private sector perspective, CREST is at the forefront of cybercrime prevention initiatives in the United Kingdom. It partnered with the National Crime Agency (NCA) in 2015, confirming the efficacy of a Cyber Criminal Career Pathway and published a joint report on its findings in 2016 (NCA/CREST, 2016), updated in 2021.

The argument for an Offender Prevention Cyber-Dependent Crime resource has been won in the UK.

There are similar projects now underway in the Netherlands and Finland. There is traction in several other countries. More than 100 government representatives from 40 countries attended NCA-led global cybercrime prevention workshops in the UK, Romania and Brazil in 2019-2020.

A further 43 countries were scheduled to attend two workshops in Asia and Africa last year, before the pandemic emerged.



Foreword

Nevertheless, the Cybercrime Prevention fire has been lit. The capacity for developing an international Prevent network is now in place and being progressed through Europol initiatives being led by the Netherlands.

It is important to state that this document is guidance - it is not prescriptive. It aims to be an off-the-shelf manual for establishing cybercrime prevention as part of a National Cyber Security Strategy or equivalent policy. This guidance provides a generic overview of the component parts that could, or should, be considered when developing an effective national template for Cybercrime Prevention. It is offender-focused and designed to work in tandem with more conventional victim-focused cybercrime prevention strategies.

The guidance is based on the author's knowledge, skills and experience of formulating national cybercrime prevention strategies in the United Kingdom and Netherlands. It outlines a template for devising, implementing, and monitoring prevention initiatives and interventions drawn from the private sector, municipalities and criminal justice system.

In this document, you will find proven mechanisms for tackling the rising phenomenon of youth cybercrime and imposing a greater law enforcement presence on the more deviant aspects of the world wide web.

It highlights the growing availability of criminal tools and normalisation of malware as a service (MAAS), necessitating prevention for all forms of cybercrime.

It is dynamic guidance, allowing for ongoing review and amendment as additional information and insights become available.

Profile

Greg Francis BEM JP
Managing Director
4D Cyber Security, Cybercrime Prevention

Greg possesses more than 25 years experience within the UK Criminal Justice System as a Specialist Investigator with HM Customs & Excise, the Serious Organised Crime Agency (SOCA) and the National Crime Agency (NCA).

He is also a Magistrate, a role he has performed since 1994.

Greg coordinated and managed the NCA Cyber Prevent Network from 2013 to 2020.

He devised and implemented many of the initiatives and interventions utilised in the UK. Greg's extensive experience as a Magistrate has generated acute insight into offending and the considerations an adjudicator must make.

He is currently Senior Consultant to the newly formed Netherlands National Police Cyber Offender Prevention Team, advising on the establishment of its Prevent programme.

Executive Summary

The United Kingdom and the Netherlands are at the vanguard of cybercrime prevention globally. They are frequently cited throughout this guidance as examples of good practice.

No advice on how to create a cybercrime prevention programme can be taken without first providing a brief overview of cybercrime, its impact on the expanding African and Asian economies and the current mechanisms in place to combat it.

Cybercrime prevention is explained by describing the historic crime prevention premise on which it was founded - and how that manifests itself in contemporary approaches to combating cybercrime. The question "Why cybercrime prevention?" is then addressed by referencing diverse types of offences - and their categorisation in terms of societal harm and impact. Cybercrime prevention and the disproportionate number of younger offenders in this space is highlighted, as are global concerns about this rising phenomenon.

Given that criminal justice systems need to balance "public service before police force," cybercrime prevention aims to ensure potential cybercriminals are given the right tools and information to make informed choices about their career path, legitimate or illegitimate.

The evolution of cybercrime prevention in the UK is documented, alongside mechanisms established to develop this approach. A spotlight is placed on the behavioural debriefs of offenders and the Cyber Criminal Career Pathway that came from those interactions, which then helped forge a template for cybercrime prevention.

"The question "Why cybercrime prevention?" is then addressed by referencing diverse types of offences - and their categorisation in terms of societal harm and impact."

Once a comprehensive review of cybercrime prevention initiatives and interventions is undertaken, the guidance illustrates the individuals and institutions needed to create a constructive, effective response.

The 4D Approach Cybercrime Prevention Model: Deter, Divert, Degrade and Disrupt, is explained. It is aligned with initiatives and interventions targeting those with potential criminal interest at the entry stage of the cybercrime pathway to committed criminals at the other.

A review of the criminal justice system and cybercrime prevention interventions designed to inhibit re-offending and promote reintegration into society is provided in this document.

The guidance goes on to propose a legislative, judicial and executive structure to implement cybercrime prevention through a government directed National Cyber Security Strategy (NCSS). Macro and micro models are provided, detailing the pivotal roles government departments can play (such as in justice, education and employment, for

Executive Summary

example). The proactive, public-facing roles police cybercrime units play in delivering prevention at executive level is detailed.

This document also provides a mechanism for managing the implementation process for establishing a Cyber Prevent programme. It includes phases outlining a scoping exercise, planning, advocacy and recruitment. Draft Prevent Officer recruitment criteria is detailed in the appendix.

The Metrics and Measurement chapter describes aspects of the Prevent portfolio that can deliver clear statistics on scope and effectiveness.

This section highlights the value of early academic engagement to determine effective performance indicators and the importance of gathering empirical evidence of cybercrime prevention tools and techniques.

The chapter also details potential difficulties in measuring the success of cybercrime prevention and explains the importance of 'Impact over volume' when assessing such programmes.

The closing chapter defines Digital Responsibility. This includes looking into central prevention themes such as self-policing, corporate social responsibility and the importance of public/private sector collaboration to help achieve a credible, sustainable cybercrime prevention model.

The guidance proposes a cyber prevention strategy as a critical, holistic approach to supplementing conventional law enforcement approaches to addressing cybercrime.

Understanding cultural and socio-economic factors, alongside insight into offender motivations and characteristics, are significant in building a sustainable cybercrime prevention programme.

Emphasis is placed on the role of ministries of justice and other key government departments to direct and deliver structural interventions through two National Prevent Officers and their domestic and international Prevent network. That aside, the significance of digital responsibility, public/private sector collaboration and societal ownership of key areas of the cybercrime problem cannot be overstated.

The guidance culminates in revealing the comparatively low resources cybercrime prevention programmes require to secure high impact.

Introduction

Cybercrime is rising. Perpetrators' technical skill is improving, and they are getting younger. This is a global phenomenon. The capacity of law enforcement agencies to bring justice to those engaging in cybercrime at all levels is outstripped by the sheer volume of those involved.

Governmental responses to cybercrime are compromised by a myriad of issues including:

- Its border-less nature
- A lack of international consensus
- Ineffective legislation, and
- Poor public awareness of cybercrime

The digital landscape is expanding with nations, individuals, institutions and industries becoming increasingly dependent on technology. Our personal lives, businesses and core services are reliant on technology like never before.

As Ian Glover, CREST President states: "A common international approach to reduce the risk of young and vulnerable people from being groomed into cyber-crime activities is essential. There is, however, a lack of any central guidance on what this approach should look like, and current good practice is not being shared on a structured basis. This guide has been written to support countries in Africa and Asia but is, in fact, much more widely relevant." (CREST, 2021).

Asia and Africa's increasing use of, and reliance on, digital infrastructure is paralleled by the increase in cyber-attacks and sophistication of threat actors. Symantec representative Bulent Teksoz highlights this growing concern: "Cybercrime is shifting towards emerging economies. This is where cyber criminals believe the low-hanging fruit is." (Kshetri, 2019).

Cybercrime prevention aims to ensure those with interests in, and/or understanding of, digital technology are made fully aware of the extensive legitimate opportunities available in education and employment within the cyber and wider technology ecosystem.

It prioritises the need to raise public awareness and deter and divert people away from cybercrime, by showing alternative pathways.

Cybercrime prevention is not a passive approach to cybercrime, it also aims to degrade and disrupt cybercriminals and their activities. It highlights the detriments of pursuing an illegitimate career online.

For individuals or groups consciously choosing a cyber criminal pathway, despite knowledge of the domestic and global necessity for such digital skills and the legal and life implications, cybercrime prevention will impact their criminal activities.

It utilises strategies to increase risk to criminals, and to compromise mechanisms facilitating cybercrime - and its dividends. Resources include partnerships with the private and public sector, international law enforcement agencies and academia.

Cybercrime prevention is of paramount importance in the battle to decrease cyber-attacks, reduce offending, focus cyber security and ensure digital talent is directed towards positive alternatives and activities.

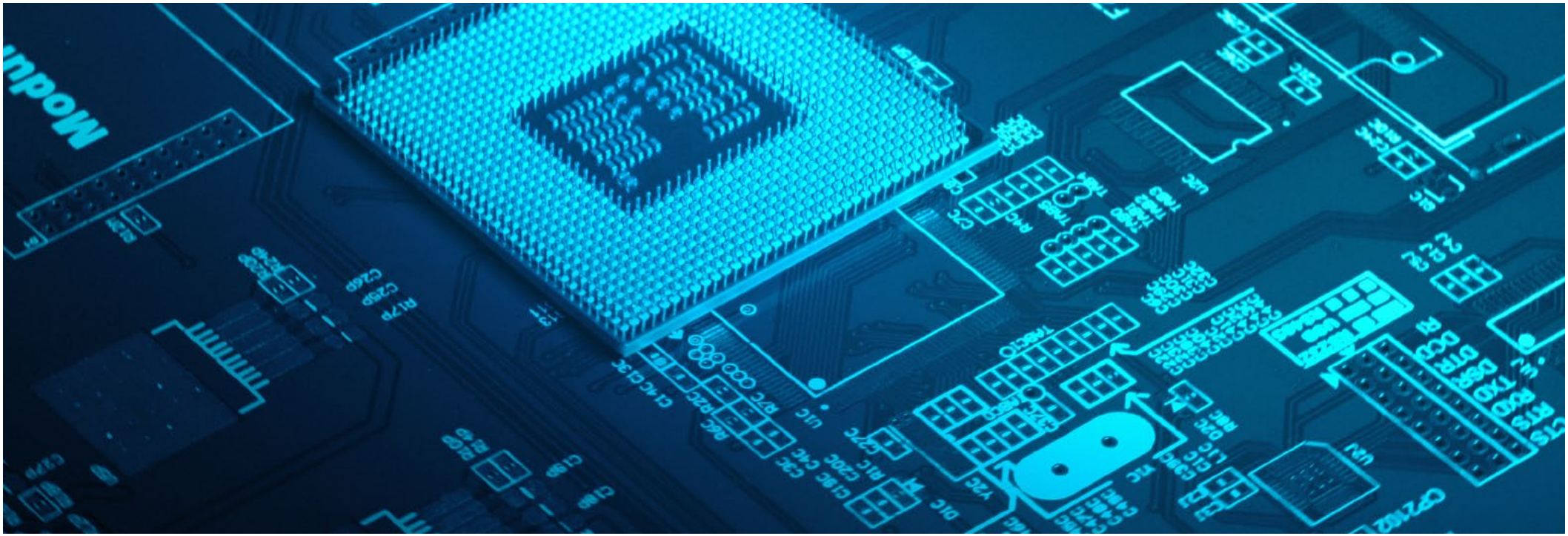
Introduction

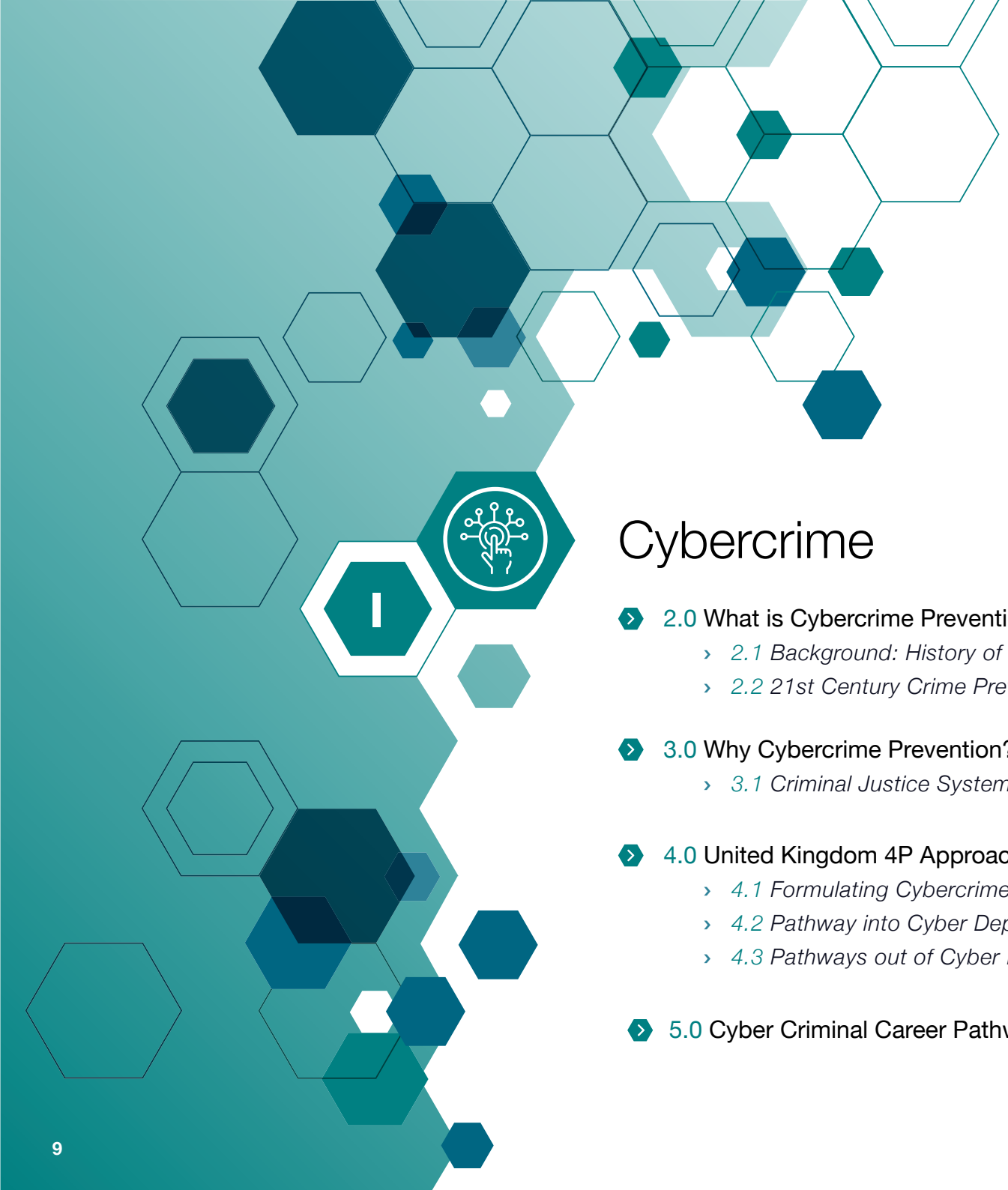
Many individuals who have started on the pathway toward cybercrime claim they were unaware of the impact of their activities. If they were aware, and understood that there are alternatives, it has been proven that the majority do not continue on the pathway. An effective, nationally directed, regionally delivered cybercrime prevention programme will prioritise 'public service before police force. This ensures everyone expressing interest or engaging in cybercrime is fully aware of the legal and life implications of cybercrime, alongside the legitimate opportunities available to utilise their digital interest, skills, and abilities.

Cyber offender prevention does not tell an individual how to conduct themselves online, rather it aims to ensure they are in a position to make an informed choice.

> *"Prevention is better than cure."*

[1] *Desiderius Erasmus, Philosopher, 1500*





Cybercrime

2.0 What is Cybercrime Prevention?

Introduction

Cybercrime is often justifiably perceived as technical offences requiring technical solutions, such as anti-virus software, firewalls and penetration testing, for example. This perception is enhanced by traditional law enforcement responses of arrest and prosecution, which aim to protect digital assets and prosecute perpetrators.

Cybercrime prevention focuses on the human aspects of cybercrime, the offender. Factors such as an offender's motivations, behaviours and characteristics are considered when determining responses to online crime. Those tasked with cyber security at the highest levels recognise that social sciences can, and should, play a significant role in tackling cybercrime.

As Douglas Maughan, head of cyber security research at the US Department of Homeland Security puts it: "We've had too many computer scientists looking at cyber security, and not enough psychologists, economists and human-factors people." (Waldrop, 2016),

For cybercrime to be profitable, a wide range of non-technology-based activities must also be in place. These activities – mules and money laundering, for example - are seldom considered in discussions on cybercrime activities.

Cybercrime prevention places emphasis on understanding the ***offender*** not the ***offence***.

Prevention revolves around initiatives and interventions designed to deter and divert an individual from cybercrime, allowing authorities to focus on those committed to offending.

This approach ensures those arrested for primarily cyber -dependent crimes have already made informed choices about their actions and their implications.

Cyber-dependent crime (CDC) - or pure cybercrime – is defined under the United Kingdom's **National Cyber Security Strategy** as: "Crimes where the devices are both the tool for committing the crime, and the target of the crime (e.g., developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity)."

"We've had too many computer scientists looking at cyber security, and not enough psychologists, economists and human-factors people."

2.0 What is Cybercrime Prevention?

Introduction

Illicit hacking, denial of service attacks (DOS), viruses, Trojans, worms, spyware and ransomware fall squarely under the banner of Cyber-Dependent Crime.

Cybercrime prevention does not ignore the other widely accepted category of digital offending, Cyber Enabled Crimes (CEC). These are traditional crimes enhanced and amplified by digital technology, enabling an increase in their reach and scale. The United Kingdom Crown Prosecution Service (2019) defines CECs as: “Crimes which do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology”.

Economic cybercrime including fraud (phishing and pharming, for example) and online marketplaces for trading illegal items are prime examples of CECs. Current manifestations of cybercrime see increasing connectivity between cyber -enabled and cyber -dependent crimes. This cross-fertilization is identified by Interpol’s ASEAN Cyber Threat Assessment 2021 report.

It outlines cybercrimes rising trajectory and partly attributes the increase to: “highly organised cybercriminals sharing resources and expertise to their advantage.” (INTERPOL 2021)This growing dynamic helps further explain cybercrime prevention’s focus on Cyber-Dependent Crime, the 4D approach advocated and detailed in a later chapter, and its trickle-down effect on Cyber-Enabled Crime.

2.0 What is Cybercrime Prevention?

2.1 Background: History of Modern Policing

2.1.1 Peel's Principles

To understand the rationale for this cybercrime prevention strategy, context must be provided, detailing the significance placed on traditional crime prevention as a central pillar of global modern policing.

According to Sir Robert Peel, the founder of modern policing: "The basic mission for which the police exist is to prevent crime and disorder." (Lentz and Chaires, 2007)

Sir Robert Peel, the 19th century British parliamentarian, is universally accepted as the architect of policing and law enforcement concepts embraced by western democracies. He placed crime prevention at the helm of his nine core principles of policing.

Peel's principles are component parts of policing models across the world. How these principles manifest in 21st century nation -states are not subject to discussion in this guidance. What is important is that the first principle, prioritising the importance of crime prevention, lays the foundation for three of Peel's principles that form core elements of the cybercrime prevention model proposed in this document.

They are as follows:

Peel's Principles	Principle Reflected in Cybercrime Prevention
Police use physical force to the extent necessary to secure observance of the law or to restore order only when the exercise of persuasion, advice and warning is found to be insufficient.	This principle reflects the notion of public **service before** police **force** ensuring that all those engaging in cybercrime have made an **informed choice**.
To recognise always that the test of police efficiency is the absence of crime and disorder, and not the visible evidence of police action in dealing with them.	Communication: Raising public awareness of cyber dependent crime and the pathways into it to promote self-policing.
Whether the police are effective is not measured on the number of arrests but on the lack of crime.	**Impact over Volume**. One individual engaged in cyber-dependent crime can cause more damage and harm than 100 arrests for traditional crime.

Figure 1: Peel's principles reflected in Cybercrime prevention (4D Cyber Security, 2021)

Peel's principles are still relevant today and helped define the rationale for cybercrime prevention described here.

These principles will be further explored and explained later, with clear illustration of how they manifest in the cybercrime prevention4D approach.

2.0 What is Cybercrime Prevention?

2.2 21st Century Crime Prevention

Crime prevention is accepted as one of the central functions of all criminal justice systems. The United Nations Office on Drugs and Crime (UNODC) states that: "Prevention is the first imperative of justice." (United Nations Office on Drugs and Crime, 2021).

That position is further explained by an Economic and Social Council statement: "Crime Prevention comprises strategies and measures that seek to reduce the risk of crimes occurring, and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes." (United Nations Office on Drugs and Crime, 2021).

Government leadership at all levels is required to create and maintain an institutional framework for effective crime prevention.

Socio-economic development and inclusion refer to the need to integrate crime prevention into relevant social and economic policies, and focus on the social integration of at-risk communities, children, families, and youth.

Cooperation and partnerships between government ministries and authorities, civil society organisations, the business sector, and private citizens are required, given the wide-ranging nature of the causes of crime and the skills and responsibilities required to address them.

Sustainability and accountability can only be achieved if adequate resources to establish and sustain programmes and evaluation are made available, and clear accountability for funding, implementation, evaluation and achievement of planned results is established.

Knowledge-based strategies, policies and programmes need to be based on a broad multidisciplinary foundation of knowledge, together with evidence regarding specific crime problems, their causes, and proven practices.

Human rights/rule of law/culture of lawfulness the rule of law and human rights recognized in international instruments (to which Member States are parties) must be respected in all aspects of crime prevention, and a culture of lawfulness actively promoted.

Interdependency refers to the need for national crime prevention diagnoses and strategies to take into account, where appropriate, the links between local criminal problems and international organized crime.

The historical and global framing of crime prevention both segue into the cybercrime prevention approach of the United Kingdom and the Netherlands. The approach taken provides historical evidence to support the argument for prevention to be an integrated component of national cyber security strategies, and aligns with 21st century models for tackling crime.

2.0 What is Cybercrime Prevention?

2.2 21st Century Crime Prevention

"The principle of differentiation calls for crime prevention strategies to pay due regard to the different needs of men and women and consider the special needs of vulnerable members of society."

[1] *United Nations Office on Drugs and Crime, 2021*

2.2.1 From United Kingdom Serious Organised Crime Agency (SOCA) to National Crime Agency (NCA)

The origin of cybercrime prevention as part of a coordinated national strategy for combating online criminality arose from the United Kingdom's Serious Organised Crime Agency (SOCA).

A cybercrime prevention team, created in 2011, focused on degrading and disrupting online criminal marketplaces alongside raising the on- and offline profile of the "cyber police" through its interventions at all levels of cybercrime.

It primarily focused on high volume, cyber-enabled crime. Between 2012 and 2013, there was a transition from one national law enforcement entity, SOCA, to its new manifestation, the National Crime Agency (NCA). Within the new National CyberCrime Unit (NCCU) investigation was re-aligned from 'cyber-enabled', traditional crimes enhanced by digital technology, to 'cyber-dependent' crimes; new crimes that need and use technology solely to cause harm to technology and those using it.

3.0 Why Cybercrime Offender Prevention?

Introduction

There is global consensus that cybercrime - along with terrorism and espionage - is one of the most serious concerns for nation-states. Incidents of significant cybercrime are increasingly more in the spotlight, from reports of hostile state action and corporate ransomware attacks to recreational hacking.

Here lies the essence of cybercrime prevention's emphasis on Cyber-Dependent Crime. There is a real and present danger to national security by those who have the technical knowledge, skills, understanding and determination to compromise digital infrastructure, penetrate sensitive networks, destabilise essential services and, when combined with social engineering, endeavour to manipulate the masses.

In the UK, the Centre for the Protection of National Infrastructure (CPNI) recognises the effects of such targeted activities. It states: "Cyber security affects both the public and the private sector and spans a broad range of issues related to national security, whether through terrorism, crime or state and industrial espionage… some individuals and groups use cyberspace for malicious purposes." (CPNI, 2021)

Interpol prioritises Cyber-Dependent Crime, including malicious domains, ransomware, data-harvesting malware, botnets, crypto-jacking, darknet and cybercrime as a service. With membership of 190 countries, Interpol ensures its knowledge, resources and insights afford members the best possible information to reduce the harm and impact of cybercrime in their countries.

> *"Interpol prioritises Cyber-Dependent Crime, including malicious domains, ransomware, data-harvesting malware, botnets, crypto-jacking, darknet and cybercrime as a service."*

Interpol states: "Criminals use new technologies to commit cyber attacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide." (INTERPOL, 2021 (2)).

Interpol's Global Cybercrime Strategy reinforces the focus on Cyber-Dependent Crime (pure cybercrime) declaring that: "The primary scope of Interpol's Cybercrime Programme is to target "pure cybercrime", crimes against computers and information systems where the aim is to gain unauthorized access to a device or deny access to a legitimate user (typically thorough the use of malicious software)." (INTERPOL, 2017).

It is only in this realm of hacking and malicious software development and deployment that a single person (and from a typical prevent perspective, a teenager), can cause significant damage to individuals, institutions and infrastructure. Their activity can be deemed so serious that national and international law enforcement must be engaged. For example, an investigation can move from the NCA to the FBI to Interpol and others for a global response.

3.0 Why Cybercrime Offender Prevention?

Introduction

Casey Crane, in a 2020 article '**Hashed Out by the SSL Store**' reports that: "some of the biggest cybercrimes in 2020 and in recent years have been pulled off by individuals who weren't old enough to graduate high school…"

Crane further acknowledges this group's capability to cause harm through: "...sophisticated cybercrime-attacks that have impacted thousands of people and resulted in millions of dollars in indirect and direct losses."

> *"There are hundreds of tutorials and digital manuals that explain, step-by-step, how to access computers or steal passwords… in environments, social media and websites linked to teen-oriented content."*

[1] *Revelock 2019*

Psychological research into teenage emotional development describes those years (12-20) as a prime time for impulsiveness, low self-control and risk-taking. Research re-enforces the point by identifying the harm young people can cause if unaware of the full implications of their actions. Technically skilled young people invariably cannot be regulated by those charged with doing so: "It is important to educate children and young people on the dangers of such activities, as research suggests that many do it for a sense of fun without realising the consequences of their actions, or the severe custodial sentences that can result." (Livingstone et.al, 2017).

The NCA's National Cybercrime Unit found that 61% of computer hackers identified in the United Kingdom began illegal online activity before they were 16 years old.

This dynamic is not in isolation. Australia's Bureau of Statistics and Crime Investigation, reporting on cybercrime in 2015, indicates the same correlation: "Crimes committed by under-18s had risen by 26% in the previous two years and by 84% in the previous three." (Livingstone et.al., 2017).

As can be seen, it takes time for research and statistics to filter through the system but the landscape changes very quickly. From research CREST has conducted it is clear that while the traditional "hacking for fun" model still exists, cyber criminals are looking to recruit more young people into the industry by promoting stories of how much money can be made and the lifestyle that can be achieved.

To compound matters further, technical proficiency is not necessarily a requirement for inflicting significant digital harm. A plethora of cheap, if not free, hacking and related paraphernalia is available for anyone interested via the internet.

It is in this area we find a disproportionate amount of 'script kiddies.' This derogatory term, coined by the hacking community, describes young individuals with little, if any, real technical understanding or skills. The 'script kiddie' uses tools and techniques developed by others to cause harm, impress friends, gain favour and hopefully credibility within online communities.

"There are hundreds of tutorials and digital manuals that explain, step-by-step, how to access computers or steal passwords…in environments, social media and websites linked to teen-oriented content." (**Revelock, 2019**).

More recent research suggests tools are also becoming more accessible and more sophisticated. For example, there has been a rise in tools designed to extract money from cybercrime activities.

3.0 Why Cybercrime Offender Prevention?

3.1 Criminal Justice System

3.1.1 Aggravating/Mitigating circumstances

Cybercrime prevention is not social work.

It is primarily police work, supported by public and private sector partners. Social work and cybercrime prevention are two distinct areas where there may be some crossover, but ultimately prevention is a mechanism within the criminal justice system to protect the public from harm.

It places emphasis on 'Service before Force' to ensure that, on arrest, law enforcement can prove that an individual has received a warning notice through:

- An Adword warning campaign
- A 'Cease and Desist' visit
- An 'Influence Activity' warning email
- Cybercrime prevention modules for schools,
- or any other Prevent intervention

These interventions will be explained in later chapters. Their aim is to reduce - if not nullify - any "no knowledge" mitigation offered by the individual on arrest, or a lawyer in their defence.

Once subject to a prevent intervention, no one should be able to say they were unaware of the illegality and implications of their behaviour.

They will then justifiably be subject to the full weight of the law.

Most importantly, significant time and money is not wasted by law enforcement investigating and prosecuting cases that are unable to reflect (in sentencing) the harm and damage caused by the criminal act because of credible mitigation.

3.1.2 United Kingdom: National Crime Agency

The National Crime Agency (NCA) has had a cybercrime prevention programme in place since 2013. It investigates, arrests and prosecutes criminals for Serious Organised Crime (SOC).

The House of Lords Library defines SOC as follows: "Criminal activity that is planned, coordinated and committed by people working individually, in groups, or as part of transnational networks. It usually centres on acquiring money, profit, influence and power."

This includes drug importation, human trafficking, economic crime and cybercrime. In 2019, it reported the average age of arrest for traditional serious crimes is 37 years old. The National Cybercrime Unit (NCCU), which investigates primarily cyber-dependent crime at the highest level, provided an average age of arrest as 19 years old.

Reference to the United Kingdom NCA is significant for planning and implementation of a cybercrime prevention programme. Until 2020, the UK was the only country with a government-directed, police-delivered prevent strategy.

3.0 Why Cybercrime Offender Prevention?

3.1 Criminal Justice System

There is a fully funded team of officers, at national and Local level, to implement it. Understanding the rationale for the UK cybercrime prevention strategy is central for any nation state when formulating their own strategy. It will enable countries to tailor their own prevent programmes and determine what aspects are transferable and what are not.

We need cybercrime prevention because of a multi-pronged scenario, comprising:

- Young, digitally able cybercriminals
- Irresponsible hobbyist hackers
- Largely unregulated cyber space, and
- Significant Lower-level crime, which escalates if left unchecked

The situation is compounded by poor public cyber-dependent crime awareness, a paucity of on- and offline technical development resources, and a criminal justice system misaligned with understanding of the digital world.

When these factors converge, too often they culminate in significant harm on national and international scale and the arrest of individuals, (who could have been deterred or diverted if they had received a credible intervention at the appropriate time), by the appropriate individual or institution.

The next chapter details the evolution of cyber-dependent crime prevention strategy and highlights milestones in the journey to formulate a holistic response to the global rise in cybercrime.

"The National Cybercrime Unit (NCCU), which investigates primarily cyber-dependent crime at the highest level, provided an average age of arrest as 19 years old."

4.0 United Kingdom 4P Approach

4.0 Introduction

The UK National Crime agency led development of law enforcement cyber prevention strategy. The NCA investigative model uses a ground-breaking concept, originally devised for counter terrorism, known as the 4P Approach: Prepare, Protect, Pursue and Prevent.

The diagram below (created by the UK College of Policing, 2020), outlines the 4Ps:

Figure 2: Outline of 4P Approach (UK College of Policing, 2020)

Prevent, required a template for how this strand of the 4P Approach was to be built into the NCA National Cybercrime Unit (NCCU) as directed by the government's national cyber security strategy.

The NCCU had a blank canvas - so a strategy for Prevent had to be conceptualised, developed and delivered.

4.1 Formulating Cybercrime Prevention: Behavioural Debriefs

With a remit to deter and divert individuals from primarily cyber dependent crime, the newly-formed NCCU prevent team conducted several debriefs with individuals guilty of serious cyber-attacks that warranted the development/deployment of malicious software (such as viruses, worms, Trojans, spyware, rootkits and Botnets).

Individuals gave their time willingly, without provisos or offers of favourable treatment from the criminal justice system or third parties. They were stimulated by the possibility that their life stories could prevent others becoming embroiled in cybercrime without understanding the consequences on their future expectations and aspirations. They saw themselves as people who would have benefited from such an initiative.

The debriefs were conducted as informal interviews with a purpose. Questions were constructed to identify commonalities, characteristics, interests, traits, and behaviours with an emphasis on determining the person's journey from digital interest to serious cybercrime.

4.0 United Kingdom 4P Approach

4.2 Pathway into Cyber Dependent Crime

The subjects all showed interest in how digital technology worked, from as early as eight years old.

They shared the following characteristics and experiences:

- Male (under 23)
- Technically proficient (coding, programming etc)
- Motivated by technical challenges, problem solving and online reputational enhancement
- Disconnected and/or disinterested from conventional education
- Disinterested and disengaged from offline activities
- Unregulated in their digital learning
- Socially awkward, or neurodiverse (Autism, Asperger's, ADHD etc)
- Parents/guardians unable to access and/or manage their online environment
- Dearth of public awareness of cybercrime and computer misuse legislation
- Absence of key criminal motivators such as money or malice
- First time offender

4.2.1 Gaming: Modding and Cheating

The unauthorised modifying ("i.e. modding") of, and "cheating" at video games is the introduction and first step on the pathway for most youth to the illegitimate side of the digital world. This is not to say that gaming leads to cybercrime. Millions game globally without any criminal inclination or engagement in illegitimate activity. 'Modding' or 'mods' can be described as, "changes made by a user or owner to a programme, object or device, in order to change its appearance or function." (Cyber definitions, 2021).

To establish how modifications and cheats are developed, interviewees said they engaged in forums, YouTube videos and other online mediums to gain and share knowledge and insights. Collectively, they professed aptitude for the technical aspects of gaming and dived head-first into programming, coding and related activities.

The NCA Pathways into Cybercrime intelligence assessment (National Cyber Crime Unit Prevent Team, 2017) provides anonymous segments from the debriefs that support the pathway. It states that: "Subject 1 enjoyed meeting other gamers and enjoyed building his credibility with them. He was motivated to build a good reputation in his gaming community. He began to frequent more forums…," quoting: "I was driven by my curiosity, I wanted to understand the best modifications and cheats."

4.2.2 Hacking Forums

The interviewees' initial enthusiasm for developing gaming cheats soon waned. They then admitted to seeking more technical challenges and problems to solve - and with that came increased self-esteem and sense of value.

The hacking community provided a fertile, unchartered, unfettered landscape. It offered infinite challenges and generated an intoxicating desire for reputational enhancement from online peers.

With little to no discussion, understanding or concern of where the boundaries were between legal and illegal, they found themselves moving from the periphery into more serious aspects of cybercrime: "…there was a relaxed atmosphere. We felt at ease discussing botnets and other hacking tools." (National Cyber Crime Unit Prevent Team, 2017)

By drilling into these human aspects of cybercrime, clear and concerning factors came from the debriefs.

4.0 United Kingdom 4P Approach

4.3 Pathways out of Cyber-Dependent Crime: Law Enforcement

All subjects debriefed by law enforcement stated they would have discontinued their criminal activities if they had received an intervention advising them of relevant legislation and the full effects of their actions on others and themselves if caught.

There was consensus that if, during their passage to cybercrime they were directly targeted with a notification such as a pop-up, warning email or 'Cease and Desist' visit from law enforcement they would have disengaged from any illegal activity.

The NCA Pathways report quotes a supporting view: "Subject 1 claimed a warning from law enforcement would have made him stop his activities. He felt that there should be more regulation of forums like **Hackforums.net**." (National Cyber Crime Unit Prevent Team, 2017)

The subjects took comfort in the low perception of risk, online anonymity and the significant numbers of people openly engaged in all forms of digital deviance and explicit cybercrime. There was little evidence to concern themselves with the clutches of the criminal justice system. Arrest and prosecution by the "cyber police" were laughed about, with the view that the "Feds" were nowhere as smart as they were.

4.3.1 Parents, Guardians, Third parties

Timely and informed interventions from parents, educators, digital industry representatives and other third parties would also have had significant merit. Subjects, to a person, were completely disconnected from their parents or guardians when it came to understanding of their online activities.

Although some parents tried to become involved, control of the digital experience was firmly in the hands of the subjects, and they knew it.

On being shown a page of binary code, mention of programming languages or attempts to discuss the merits of using one programming language over another, for example, parents were lost... but comforted by the fact that their child was a 'genius' and not wandering the streets with unsavoury characters.

As one subject puts it: "My mum was happy that I wasn't out on the streets all day and night." (National Cyber Crime Unit Prevent Team, 2017)

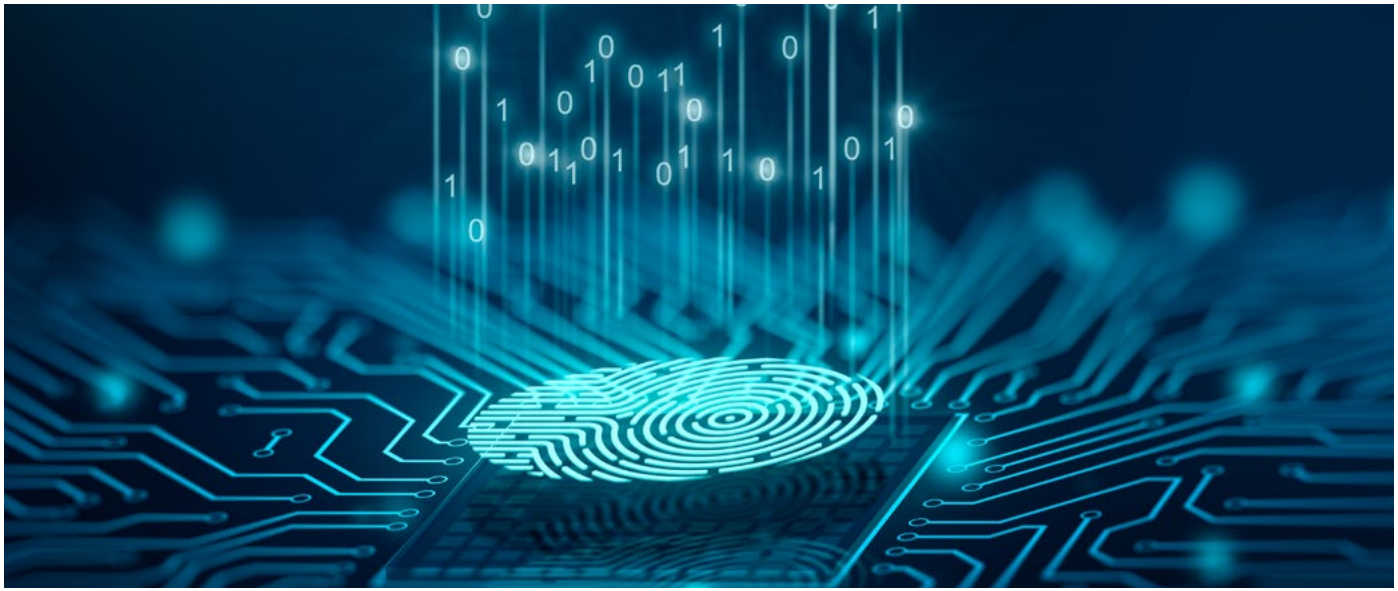
4.3 Pathways out of Cyber-Dependent Crime: Law Enforcement

4.3.2 Youth Cyber -Dependent Crime Reports

The outcome of these debriefs was the production of a compelling and insightful intelligence assessment by the NCA, Pathways into Cybercrime (National Cyber Crime Unit Prevent Team, 2017). A series of meetings and workshops with academia and CREST lead to the formulation of a public/private sector informed Cyber Criminal Career Pathway (CCCP).

The CCCP draws on the central findings of the NCA Intelligence assessment and provides key milestones in an individual's journey from interest in, or aptitude for, digital technology to committing serious cyber-dependent crime.

The Pathways into Cybercrime and subsequent CCCP reports formed the basis of the UK cybercrime prevention rationale, initiatives and interventions. There is validation of the key NCA report findings in an independently commissioned report produced by Europol in 2016, Youth Pathways into Cybercrime (Aiken et al, 2016). It states: "… [the typical adolescent hacker is an] extremely intelligent young person, probably slightly vulnerable, socially awkward and withdrawn, very keen in understanding how computers work … [they] might have a slight grievance against society if [they've] been down the black hat route; or if [they're] an ethical white hat [they] may just be doing it for the challenge, so they can get the experience at something they are good at."



"… [the typical adolescent hacker is an] extremely intelligent young person, probably slightly vulnerable, socially awkward and withdrawn, very keen in understanding how computers work..."

5.0 Cyber Criminal Career Pathway (CCCP)

5.0 Introduction

The Cyber Criminal Career Pathway highlights activities and behaviours individuals may engage in as they move into cyber-dependent crime. It details the characteristics, interests and stimuli of individuals who become interested and immersed in cyber-dependent crime.

The CCCP also describes the absence of factors that contribute to a young person's self-development, as well as online understanding and execution of online social responsibility.

They include a lack of:

- Regulation/explanation of online low-level criminal activity such as, booting or DDOSing
- Interest and/or understanding of the implications of illegal online activity
- Knowledge of legislation governing the internet
- Parental/adult understanding and/or interest in a child's digital knowledge, skills and abilities
- On- and offline resources for interested youngsters, such as coding or technology clubs
- Law enforcement presence and societal value systems at all stages of online deviant activity
- Access to computer science at many schools

The CCCP does not profess to be a 'one size fits all' assessment, but it does illuminate some interesting commonalities that have been largely unchallenged by all those who inhabit the digital world.

The Pathway in its original form is outlined on the following page:

Figure 3 Illustrates the pathway from legitimate digital engagement to serious cyber-dependent crime. This coincides with a movement away from tangible real-world interactions towards immersion in virtual relationships. These online relationships are with entities engaged in technically challenging, reputationally enhancing and progressively illegal activities.

Although largely still relevant, there have been some insightful developments regarding the CCCP and Intervention points, since the diagram was drafted in 2015. An updated version is presented in a later chapter. However, the model is still credible and the primary reference point for much of the cyber -dependent prevention activity.

5.0 Cyber Criminal Career Pathway (CCCP)

5.0 Introduction

Figure 3/4: Pathway into Cybercrime (NCA/CREST, 2015)

5.0 Cyber Criminal Career Pathway (CCCP)

5.0 Introduction

The NCA Pathways into Cybercrime intelligence assessment is the only body of work where convicted, prolific, cyber-dependent criminals have actively and willingly contributed to understanding of their offending and given insights to prevent re offending, entry and immersion in cybercrime.

Key aspects of an individual's journey - from criminal interest to entry, and escalation into a serious offender - have been identified.

Measures for curtailing progression, continuance and adherence to cybercrime have been developed.

Emphasis is placed on deterring and diverting young people (that is, those 12-24 years old) away from online deviance to more legitimate and productive use of their skills and abilities.

Although the sample group of subjects interviewed is small, that does not offset the fact that five years after the interviews and research, the model still holds up well in the academic, law enforcement and hacking communities.

The NCA "Pathways" intelligence assessment and its product, the Cybercrime Cyber Criminal Career Pathway, provide the "Pillars of Prevention" for cyber-dependent crime globally.

"Emphasis is placed on deterring and diverting young people (that is, those 12-24 years old) away from online deviance to more legitimate and productive use of their skills and abilities."

Prevent Model

6.0 Prevent Model

6.1 4D Approach: Deter, Divert, Degrade, Disrupt

A '4D Approach' for development and implementation of cybercrime prevention within national cyber security strategies is recommended for the countries this guidance targets. It is a convergence of current national cybercrime prevention strategies, academic research, recent offender debriefs, criminal justice models and the CMAGE in country assessments.

6.1.1 4D Approach definition

Deter and ***Divert*** those on the periphery of cybercrime, ***Degrade*** and ***Disrupt*** those committed to cybercrime".

Deter
Raise awareness of legal and life implications of cybercrime. Increase perception of risk for online illegal activity

Divert
Illuminate legitimate opportunities in education and employment for those with technical skills and/or interest, to facilitate informed choices

Degrade
Undertake covert and overt projects that compromise the profiles, products and platforms utilised by committed cybercriminals and the infrastructure required to operate effectively

Disrupt
Work in collaboration with operational teams to triage law enforcement cyber activity and undertake arrests at all levels alongside off- and online Prevent activities

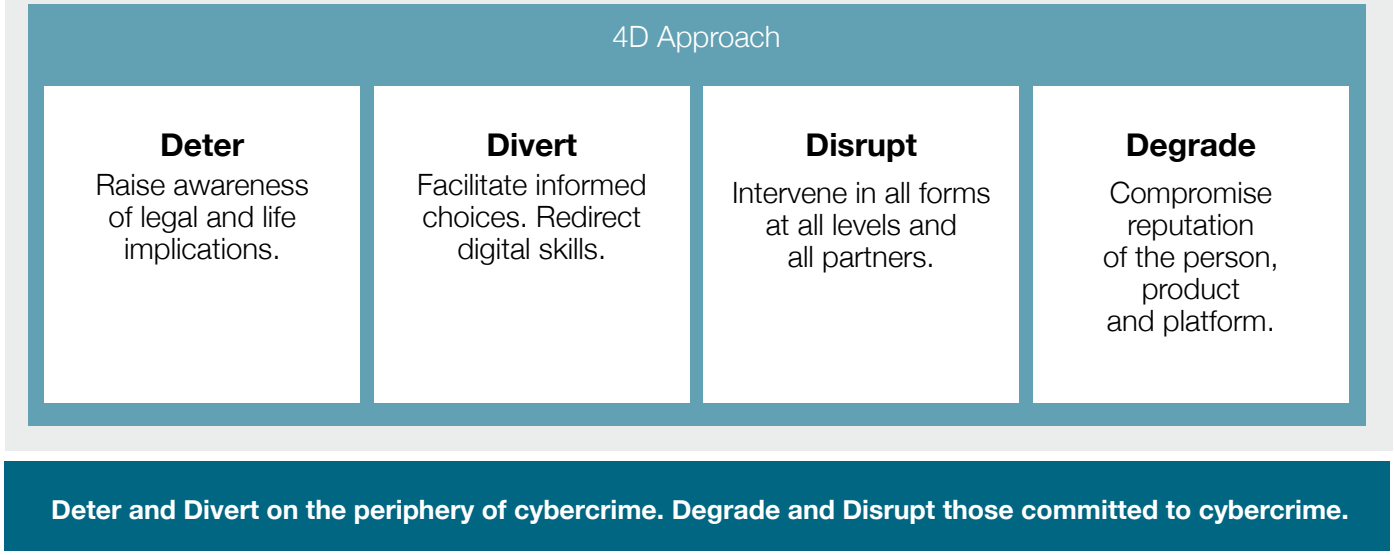


Figure 5: 4D Approach - Deter, Divert, Degrade, Disrupt (Copyright 4D Cyber Security Limited)

6.0 Prevent Model

6.2 Initiatives and Interventions - Law Enforcement (Police)

A portfolio of initiatives and interventions that can, without significant modification, be incorporated into national cybercrime prevention models have been developed since 2011. They have proven to be innovative and effective and can be tailored to accommodate cultural nuances, as well as political and socio-economic factors.

The Prevent Officer(s) based within law enforcement will be at the vanguard of delivering prevent activity. They will assess individuals and operations to determine whether they meet the criteria for a prevent intervention. An overview of the portfolio of cybercrime prevention interventions utilised are detailed below alongside the respective 4D emphasis. Where there is no compromise to sensitive law enforcement methodology, an example of how the intervention manifests in the cybercrime arena is provided.

6.2.1 Deter/Divert Criminal Interest – Words of Advice

This is the offline starting point for a Prevent Officer and their interaction with the primary target audience. “Words of advice” are simply a Prevent Officer or another person in a position of authority providing information on the negative implications of cybercrime and the legitimate opportunities available in cyberspace.

Situation
A Prevent Officer delivers a presentation to a high school assembly on Cybercrime Prevention. The IT teacher asks the officer to speak to a child from the Computer Science class who has been asking concerning questions about certain illegal activities on line.

Action
The Prevent Officer arranges to speak with the individual about the illegal detriments and legal benefits of the same digital interests and skills.

Outcome
The individual has now had direct engagement with the Prevent Officer, the school is aware and the parents advised that their child has an interest in digital technology and are provided with information that enables them to progress their interest safely and legitimately.

Figure 4: Words of Advice example - situation, action, outcome.

6.2.2 Deter/Divert Criminal Interest or Entry level intervention – Google Ads/Online Advertising Campaign

On reviewing the Cyber Criminal Career Pathway (CCCP), it was clear there was no entry level interventions for those thinking of, or starting on, their cybercrime journey. The subjects debriefed agreed they were unfettered online and would have relished the opportunity to make informed choices at the earliest stages of their exploration of the digital landscape. They professed to having little, if any, understanding, interest or concern about whether their activities were right and wrong and the potential implications of their behaviour.

Search engine-based advertising campaigns aim to fill that gap by providing immediate notification to an individual enquiring about questionable, if

not criminal, online activities of the legal status of the searched term. From a cybercrime prevention perspective, this entry-level intervention facilitates promotion of the core criminal justice tenet, 'public service before police force'. Such campaigns provide deterrent and diversionary information by highlighting the implications of continued engagement in the searched activity.

6.2.2.1. How does it work?

Search engines such as (but not limited to) Google, Bing and Yandex return warnings and information on legislation from law enforcement for criminal terms and activities searched.

The search engine analytics are tailored to a specific target audience (12-24 years old). For example, a 17-year-old searches for, "How do I DDOS?" and receives a warning message from the police co-badged with Interpol informing them of the illegality of their activity and providing information on legitimate use of their enquiry - and resources available to develop appropriate skills.

6.2.2.2 Cost

Search engine providers tend to charge on a cost-per-click (CPC) or pay-per-click (PPC) basis - the more clicks, the less cost per click.

6.2.3 Intervention - Cease and Desist

The activity warrants the signing of an official "Cease and Desist" letter by the perpetrator and awareness of the arrests undertaken by operational teams for more prolific offenders.

If age or situation is appropriate, a parent/guardian will be present and made aware of the reason for the visit, and implications of continuing along the pathway. Information is provided on cybercrime legislation, alongside legitimate opportunities for education and employment in the digital landscape.

Cease and Desist visits should be considered as an option for early intervention when:

- An individual has been identified as on the periphery of involvement in cybercrime, or
- An officer considers the conduct of an individual justifies law enforcement intervention, but the conduct has not met the threshold for arrest and prosecution

The criteria are not prescriptive. There may be several factors that influence an officer's decision as to whether Cease and Desist visits are appropriate, including:

- An individual's age
- Strength of evidence
- Seriousness of alleged criminality
- Level of harm caused
- Public interest in pursuing the alleged criminality
- The perceived receptiveness of the individual to early intervention and positive diversions

6.2 Initiatives and Interventions - Law Enforcement (Police)

A profile of the intervention follows:

Situation
A primarily online Operation with a high number of individuals affiliated through interest or actively through purchase/use of a criminal tool. The tool can be criminal by default i.e. low level DDOS tool or explicitly criminal, Remote Access Tool (RAT).

Action
Cease and Desist by primarily local police coordinated by the National Prevent Officer.

Arrest
For amplification of impact the online activity should be aligned to an offline arrest(s) domestically or internationally.
That information is communicated by the Prevent officer during the visit and accessible through the National Cybercrime Prevention website.

Outcomes

Facilitate Informed Choices. Reduce Mitigation Warning visit by Law Enforcement to individuals affiliated to or engaged in low Level cybercrime.

Figure 5: Cease and Desist example - situation, action, arrest, outcomes.

Cease and Desist is a "Stop and Think" action targeted at those more likely to be susceptible to behavioural change. The unexpected and unsettling real-world interaction with law enforcement is the intrinsic quality that Cease and Desist brings.

Law enforcement has deemed the intervention so impactive that it is now being trialled against certain actors involved in cyber-enabled crime such as money mules. It is also being positively referenced by other actors within the criminal justice system.

On its website, criminal defence law firm, **Renshaw Derrick**, states: "The authorities, in particular the NCA, often serve 'Cease and Desist' notices to young people who are becoming involved in cybercrime. The intention is to encourage young people to use their technology skills for legal purposes instead of cybercrime.

"If you are served with a 'Cease and Desist' notice (for example, because you purchased 'hacker tools') then you have been identified as potentially being involved in cybercrime, usually as part of a wider criminal investigation. You should immediately stop the activities stated in the 'Cease and Desist' letter. Continuing with the activities could result in further investigation and potentially criminal prosecution."

6.2.4 Intervention - Positive Diversion Workshop (Offline)

This is an offline, real-world intervention for (primarily) young people enquiring, entering or progressing into cybercrime. They could have come to the attention of the police for a low level cyber-dependent offence, such as hacking the school network, with a decision made not to prosecute. The workshops can be voluntarily attended or directed as an alternative to prosecution by the police.

Workshops are designed, through presentations, exercises and personal statements, to inform participants of cybercrime legislation, online social responsibility and the legal and life implications of a criminal pathway.

These one-day workshops offer insight into the wealth of education and employment opportunities for those with genuine digital interest, aptitude and skills. This two-pronged approach ensures all who attend can make informed choices. If they encounter the criminal justice system for the same or similar offences, then the situation would be aggravated by the fact they had attended a positive diversion workshop yet took no heed of warnings or opportunities presented.

6.2 Initiatives and Interventions - Law Enforcement (Police)

Parents and guardians are also encouraged to attend if their child is under 23 years old. Experience of delivering the workshops has identified the value of separate presentations provided to the parents in a separate room.

The parent or appropriate adult effectively receives the same content as the young people, with the opportunity to ask the subject matter experts questions.

This medium has proved both enlightening and empowering for adults.

For many, it was the first time they had real insight into their child's digital world, their potential to harm, along with capabilities to legitimately earn an exceptional living and make a positive contribution to society.

Situation
A school network/system is hacked by a student primarily for the challenge and impressing friends. The individual admits liability and is shown to be technically proficient and genuinely remorseful.

Action
The school head teacher is aware of the Cybercrime Prevention programme and contacts their local Prevent Officer. The young person and their appropriate adult attend a Positive Diversion workshop and receive presentations delivered by the public and private sector.

Outcomes

- Facilitate Informed Choices
- Reduce Mitigation
- Empower parents/guardians

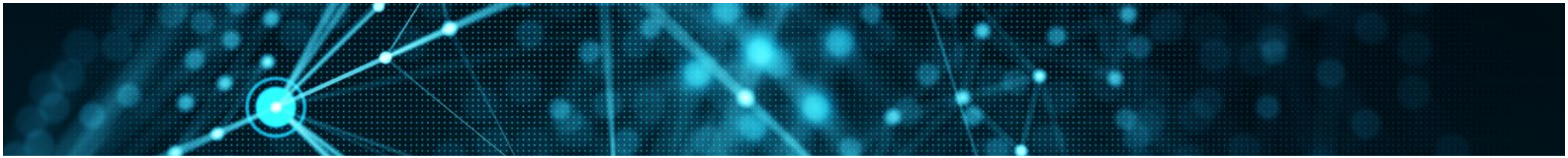
Figure 6: Positive Diversion Workshop example - situation, action, outcome

6.2.5 Degrade: Targeted intervention against committed cybercriminals

6.2.5.1. Behavioural science

'Degrade' involves efforts to compromise a cybercriminal's capability to operate by eroding credibility in their personal profiles, their products and the platforms they operate from.

Overt techniques can be used for both short and long-term impact, to sow and exacerbate mistrust and paranoia. Direct messaging onto criminal platforms by law enforcement officials is central to the effectiveness of the intervention. The platform should be blatantly discussing/prompting criminal activity and exchanging criminal ideas, tools and techniques. Law enforcement postings should advise of legislation and penalties and highlight cybercrime operations related to a particular activity.



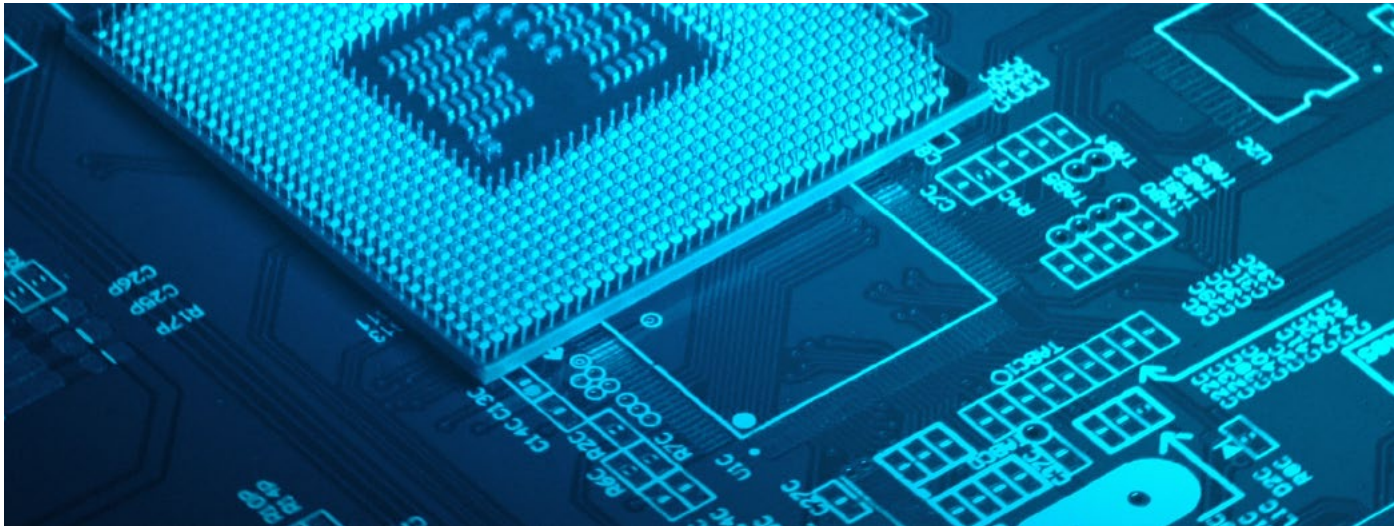
6.2.5.1. Behavioural science (continued)

This operational messaging should provide imagery of actions taken, such as infrastructure take down, arrests and house searches. This helps connect the remoteness and disconnection of virtual crime to the harsh reality of real -world consequences.

Where possible, the borderless nature of cybercrime requires this intervention to be conducted with international partners undertaking parallel activity, subsequently raising the perception of risk. The activity should be aligned to a coordinated on- and offline communications campaign, including website links to capture the user's attention. The web page advises the viewer of the operation, police agencies involved, the criminal actors arrested and infrastructure dismantled.

Below is an example of Degrade activity conducted by the Netherlands national police's national high tech crime unit in 2021. Firstly, the **EMOTET** botnet infrastructure was dismantled, and key actors arrested by the operational team.

Secondly, warning messages were posted on several English and Russian speaking forums. Validation that the message was from the Dutch police was also provided via official social media platforms.



"Overt techniques can be used for both short and long-term impact, to sow and exacerbate mistrust and paranoia.

Direct messaging onto criminal platforms by law enforcement officials is central to the effectiveness of the intervention.

The platform should be blatantly discussing/prompting criminal activity and exchanging criminal ideas, tools and techniques."

6.2 Initiatives and Interventions - Law Enforcement (Police)

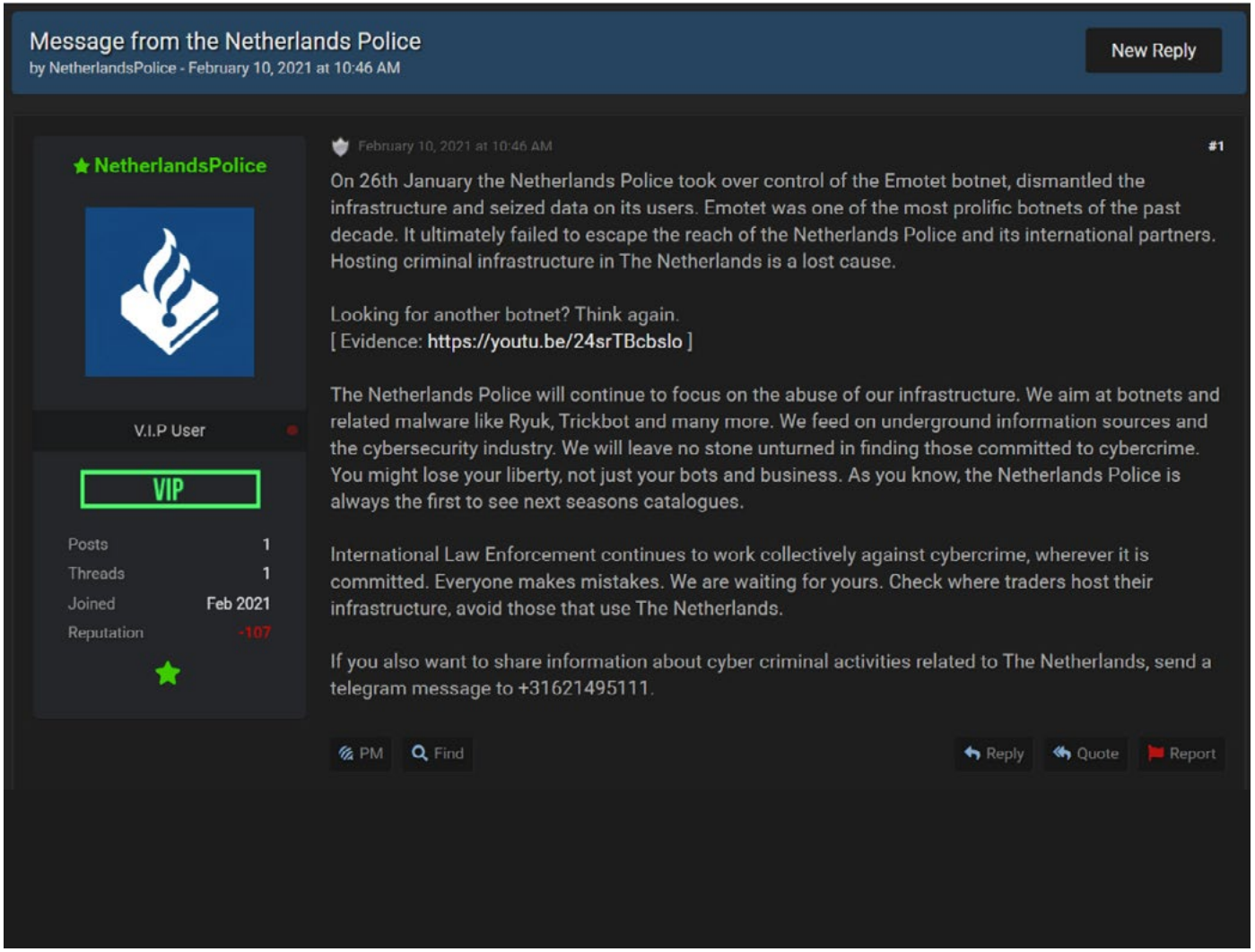


Figure 7: Netherlands National Police post on criminal forum. February 2021

6.2.6 Disrupt: Holistic law enforcement Intervention targeting all levels and both types of cybercrime with on and offline activity

6.2.6.1. High Volume action

When law enforcement dismantles criminal apparatus and arrests individuals operating within a criminal marketplace, users of that marketplace site invariably escape any direct action. Often, they simply migrate to another criminal site.

The considerable number of marketplace site users means only a small percentage of the most prolific users may be targeted for further arrests and prosecution.

This migratory effect illuminates law enforcement limitations in tackling cybercrime. However, it is possible for law enforcement to exert some impact on this type of criminal ecosystem. Where there is sufficient supporting intelligence and resources, all information gleaned from databases seized during the operation can be triaged according to the seriousness of the offence. A hierarchy of seriousness is determined by Prevent officers, with advice and direction from legal authorities.

6.2 Initiatives and Interventions - Law Enforcement (Police)

They set the criteria for interventions against lower-level offenders with arrest and prosecution at the highest end and targeted warning emails at the lower end. Further details follow:

A: Arrest and Prosecution

Regional and local law enforcement target a selection of lower-level operatives aligned to the criminal tool, website or activity, from arrest packages developed by the National Cybercrime Unit, coordinated by the Prevent Officer in tandem with the Prevent Single Point of Contact (SPOC)* network. These individuals may not have reached the threshold for National Cybercrime Unit engagement, but their criminality is significant enough to warrant police action.

B: Cease and Desist visit (see above, point 6.2.3)

This intervention is employed as a direct, explicit warning to those who have considered or committed lower-level offences. Depending on numbers, all or some of the offenders should be subject to a "Cease and Desist" visit by local law enforcement. The subject is expected to sign and retain a "warning letter" confirming their understanding of the reasons for the visit, its nature and implications of continuing their activity.

The visiting Prevent Officer also assesses the individual for additional activity that may include debriefing to further inform and improve prevention interventions or support for the parents' or guardians' activities The visit is stored on a central database to ensure records are kept and subjects receive progressive interventions if they come back into focus of law enforcement.

C: Warning email

Warning emails take the form of direct electronic message to low-level users or affiliates. A warning email should outline the law enforcement operation, with web links to the main story on a central splashpage. Such emails would only be sent if there were no details of a real-world address and insufficient intelligence or evidence to determine the most appropriate intervention for the offence(s).

The aim of the email is to unsettle and dissuade those identified as low-level from continued engagement in criminality online, by bringing the spectre of law enforcement to their world. The individuals emailed are stored on a central database to ensure records are kept.

A policy decision may be required to undertake this approach by the relevant authority within the criminal justice system. The authority would have to consider the volume of offenders, their level of offending, their inaccessibility and whether the action is in the public interest.

The value of this broad-based approach is in its disruption to the cybercriminal ecosystem. Everyone engaged on the criminal platform are impacted in some shape or form by law enforcement, unsettling widely held beliefs of law enforcement capability and raising the perception of risk, irrespective of the level of criminal engagement.

"Officers knowledgeable of cyber offender prevention tools and techniques. They are the primary reference point for any enquiries on cyber prevention. They provide guidance, identify opportunities for initiatives and coordinate interventions with internal and external parties."

6.2 Initiatives and Interventions - Law Enforcement (Police)

A review of responses from recipients of warning messages showed clear concern regarding police engagement, provoking some to deny any criminal intent and others to explain their presence on the criminal platform targeted.

6.2.6.2. Communication as a Prevent Tool

The importance of Communications for all these interventions cannot be stressed enough. A comprehensive campaign is paramount to raising awareness in our target audiences (and the public) of Pathways into cyber-dependent crime.

The UK's "**Cyberchoices**", and Dutch police's "**You are one click away from cybercrime**" campaigns were launched, and relaunched, to raise public awareness of cyber-dependent crime.

Both campaigns targeted young people and their parents and guardians by highlighting potential pitfalls online. Both shared resources online for those interested in digital technology or concerned about their child's online activity. Communication campaigns are used to illuminate the cybercrime landscape and amplify the activities to inform and direct enquiries to sources of information.

6.2.6.3. Informed choices

Cybercrime prevention initiatives and interventions are not designed to stop youngsters experimenting with, and learning about, digital technology. Society needs individuals skilled in coding, programming and other digital skills.

Cybercrime prevention is fundamentally about placing an individual in a position where they can make an "**informed choice**" about how they develop their interest and utilise their skills in digital technology.

Criminal Justice System

7.0 Criminal Justice System: Prosecution

7.0 Introduction

A criminal justice system should be able to provide exit routes from a cyber criminal pathway, particularly if an individual has been identified as suitable for an offender prevention Intervention after they have been arrested, prosecuted and/or imprisoned.

Furthermore, the CJS should have a mechanism for ensuring all involved in cybercrime are fully aware of the detrimental implications of their online criminality and have chosen to take the risk.

This section outlines some considerations for the CJS when assessing the value of cybercrime offender prevention for effective investigations, prosecutions in the public interest and purposeful rehabilitation programmes.

7.1 Investigation/Prosecution: Offset Mitigation

Cybercrime offender prevention recognises that although cybercrime prevention's primary objective is to deter and/or divert individuals from entry or progression into cybercrime, this should not obfuscate the role it can play within the investigation, prosecution and conviction of those committed to cybercrime.

Although touched on in a previous chapter, it is necessary to drill into this rationale. Within the evaluation phase, criminal justice prosecution, defence and judicial sentencing incorporates mitigating and aggravating features of the offence and the offender. Cybercrime prevention activity has been crafted to ensure individuals make informed choices about the activity they undertake online.

> *"...The CJS should have a mechanism for ensuring all involved in cybercrime are fully aware of the detrimental implications of their online criminality and have chosen to take the risk."*

Every individual should be made aware of the following:

- Online criminal activity that has come to the attention of law enforcement
- Computer-based legislation and other relevant legislation
- Implications of continuing along an illegitimate pathway
- Opportunities for legitimately utilising their skills
- Resources available to educate and develop digital interests and skills

7.0 Criminal Justice System: Prosecution

7.2 Rehabilitation: Recidivism (Re-offending)

The effectiveness and credibility of any criminal justice system is measured partly in the percentage of those detected early, and those convicted who re-offend after sentencing. The necessity for specific rehabilitation programmes to curtail progression into more serious cybercrime - and reduce re-offending for those found guilty of specifically cyber -dependent criminal offences - is paramount.

It is essential that the CJS has rehabilitative options for all offending to try and offset recidivism.

Every offence committed in the offline world from shoplifting to terrorism has bespoke rehabilitation options. While they will differ from country to country, they are present.

This has not been the case for online offending, particularly our targeted area of cyber-dependent crimes. Punishment in isolation does not necessarily stop re-offending and the cycle of offending, arrest, prosecution, imprisonment, release, offending.

Too often, this pattern is indicative of the lives of so many serial criminals.

Cyber-dependent criminals with technical skills and abilities, or the aptitude to attain them, can be reintegrated into society through legitimate employment in the digital industry, with appropriate controls and industry support.

There is abundant evidence of this happening in several countries.

“Every offence committed in the offline world from shoplifting to terrorism has bespoke rehabilitation options. While they will differ from country to country, they are present.”

7.0 Criminal Justice System: Prosecution

7.3 Hack_Right

This is a pioneering initiative developed by the Dutch national police cybercrime prevention team. An individual who has admitted guilt to a Cyber-Dependent Crime is directed by the court to the Hack_Right programme. Here, a combination of law enforcement and industry professionals provide them with knowledge required to change their lives.

They are given personal insight into the digital industry and reminded of the poor choices they made to ensure they have full awareness of the implications of further offending.

Journalist Stephen Pritchard, in an article on **Hack_Right**, makes the following observations:

Hack_Right begins to rebalance the offline and online judicial scales. It not only provides the CJS with a bespoke, credible intervention, but helps align rehabilitation opportunities for online offending with offline offenders, who have a myriad of options. The private sector play a key role,providing knowledge and guidance on the digital sector and the opportunities available.

"These initiatives work best when they are integrated with those that demonstrate proper career paths, and that you can earn as much, if not more, on the right side of the law," said Ian Glover, president of industry body CREST (Pritchard, The Daily Swig, 2020)

The programme is overseen by the Probation Service and the Prevent Officer.

"All too often, these offenders fail to realise the consequences of cybercrime. At the same time the Dutch believe that standard criminal sentences – such as jail time or fines – do little to prevent re-offending. The focus of Hack_Right is both to discourage cybercrime and encourage young offenders to move to legal activity, such as ethical hacking."

0 *Pritchard, The Daily Swig, 2020*

7.0 Criminal Justice System: Prosecution

7.4 Intervention Panels

An intervention panel initiative was developed in the UK by the counter terrorism prevent team to manage those on the periphery of radicalism. Intervention panels are now being piloted for cyber -dependent criminals who have been assessed as capable of, or have caused, significant harm.

An individual is referred by a parent/guardian, educator, Prevent Officer or judge to a panel of professionals that may include representatives from social services, cybercrime prevention, probation, youth justice teams and cyber security professionals.

The Intervention Panel reviews the individual's personal circumstances and determines the best intervention for them. They may be given support for mental health, education or social skills development, as well as access to an online portal where they can develop and progress their technical (coding) skills and engage with potential employers.

The essence of the programme is to address underlying causes of criminal intent or action; make clear the detriments to the criminal pathway and preserve talent for redirection to legitimate activities. This programme is coordinated by the Probation Service and/or the Prevent officer.

Intervention panels also provide the opportunity to debrief post-sentencing. This is a component part of the Prevent Officer's role to ensure they are continually informing and updating the Cyber Criminal Career Pathway. The importance of instinctively knowing who to approach for a debrief is a key attribute of a Prevent Officer's skills and experience. They may review a report about an individual who receives 'Words of Advice' and deem it necessary to debrief them or be assigned to debrief a person by the Intervention panel.

7.0 Criminal Justice System: Prosecution

7.5 Department Responsible For Education

A Cybercrime awareness module should be advocated by the department responsible for education. Good practice would be to incorporate a cybercrime prevention module into generic life-skills learning, specifically where digital technology is taught.

This CSR outreach could offer advice, opportunities and activities such as scholarships, tech clubs and mentoring. Such schemes can lead to encouraging and developing individuals with the right skills to fill job vacancies in the digital sector. The importance of employment opportunities and the role the private sector can play in cybercrime prevention is more comprehensively addressed in the “Digital Responsibility” section of this guidance.

7.6 Department for Employment

The cybercrime prevention “ask” is for the digital industry be made aware of the Prevent remit, and to pro-actively add a corporate social responsibility (CSR) strand to business models.

This CSR outreach could offer advice, opportunities and activities such as scholarships, tech clubs and mentoring. Such schemes can lead to encouraging and developing individuals with the right skills to fill job vacancies in the digital sector.

The importance of employment opportunities and the role the private sector can play in cybercrime prevention is more comprehensively addressed in the “Digital Responsibility” section of this guidance.

7.0 Criminal Justice System: Prosecution

7.7 Pathways into Cybercrime – Author's Update

An updated version of the 2015 Pathway is outlined below based on current insights from academia, industry and law enforcement and the current initiatives and interventions explained in this chapter.

Click to view

	Potential intervention points															
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Digital interest	●	●	●													
Computer gaming			●	●												
Online gaming	●		●	●												
Booting (DDoS)*	●	●	●	●	●	●	●									
Computer gaming modification and cheats	●		●		●	●	●	●								
Hacking forums			●		●	●	●	●		●						
Minor cybercrime challenge			●		●		●	●		●						
Cybercrime											●	●	●	●		
Serious cybercrime											●			●	●	●

Legal

Illegal

* Booting (DDoS) has been placed earlier in the pathway despite the illlegality, due to the low level of technical skill required resulting in an earlier stage of entry.

Figure 8: Pathways into Cybercrime, Author's Updated Pathway

Prevention

- 8.0 Cybercrime Prevention National Structure: Legislature, Judiciary, Executive
  - *8.1 Legislature: Government - National Cyber Security Strategy (NCSS) OR Equivalent*
  - *8.2 Judicial: Ministry of Justice*
  - *8.3 Cybercrime Prevention Officer/Prevent Network*
  - *8.4 Departmental - Ministry of Education*
  - *8.5 Ministry of Employment/Skills*
  - *8.6 Executive: Police*
- 9.0 Prevent Officer - Strategic
  - *9.1 Working Groups (WG) - Ministry of Justice*
  - *9.2 Working Groups (WG) - Ministry of Education and Employment (Skills)*
  - *9.3 Communications*
  - *9.4 Research*
  - *9.5 Child Exploitation and Online Protection (CEOP)*
- 10.0 Prevent Officer - Operational
  - *10.1 Operations*
  - *10.2 Interventions*
  - *10.3 Projects*
  - *10.4 National Outreach*
  - *10.5 Prevent SPOC Network*
  - *10.6 International Prevent SPOC Network*
- 11.0 National Cybercrime Prevention Implementation Strategy
  - *11.1 Phase One: Scoping Exercise*
  - *11.2 Phase Two: Recruitment, Advocacy, Planning*
  - *11.3 Phase Three: Implementation*

8.0 Cybercrime Prevention National Structure:

8.0 Introduction

In this section we examine the trajectory set out for devising, developing and delivering Cybercrime Prevention from a strategic level.

For the successful integration of "in country" cybercrime prevention portfolios, a structured implementation process must be devised and directed. The objectives of a Cybercrime Prevention programme need to be outlined within government policy and a ministry, or ministries, directed to implement it effectively and universally.

Academic insight has contributed to the formulation of a national cyber prevention programme. Leukfeldt and Holt (2020), in their analysis of the dynamics of cyber offending, state: "These crimes are committed by individuals or networks of people which prey upon human victims and are detected and prosecuted by criminal justice personnel.

As a result, human decision-making plays a substantial role during an offence, the justice response, and policymakers' attempts to legislate against these crimes."

The following factors will help ensure an effective, stable cybercrime prevention programme in the targeted countries:

- Assess and tailor a Cyber Criminal Career Pathway to reflect the political, cultural and socio-economic nuances of the region
- Develop a domestic and regional prevent network of government representatives, law enforcement officers and digital industry specialists
- Identify, formulate and implement an International Prevent programme as proof of concept for other regional countries
- Engage respective criminal justice systems and private industry representatives, domestically and internationally, to raise awareness of cybercrime and implement positive diversions
- Build the law enforcement infrastructure and develop interventions and initiatives fit for an evolving digital economy
- Incorporate Cybercrime Prevention modules into computer science and other relevant subjects across academic institutions at all levels

The three arms of government - legislature, judiciary and executive – must work together to ensure connectivity between cybercrime prevention policy and Prevent Officer practicality.

The ministries and departments outlined on the following page will no doubt have different names in different countries, but the specifics of the relevant Prevent component are placed in brackets to ensure correct ownership.

8.0 Cybercrime Prevention National Structure:

8.1 Legislature: Government - National Cyber Security Strategy (NCSS)

If not already clearly stipulated within a country's current cyber security strategy, a Cybercrime Prevention Programme should be established, then outlined as a core component. Without this encouragement and support from central government, it will be difficult to coordinate and encourage all the component parts necessary for implementation to work.

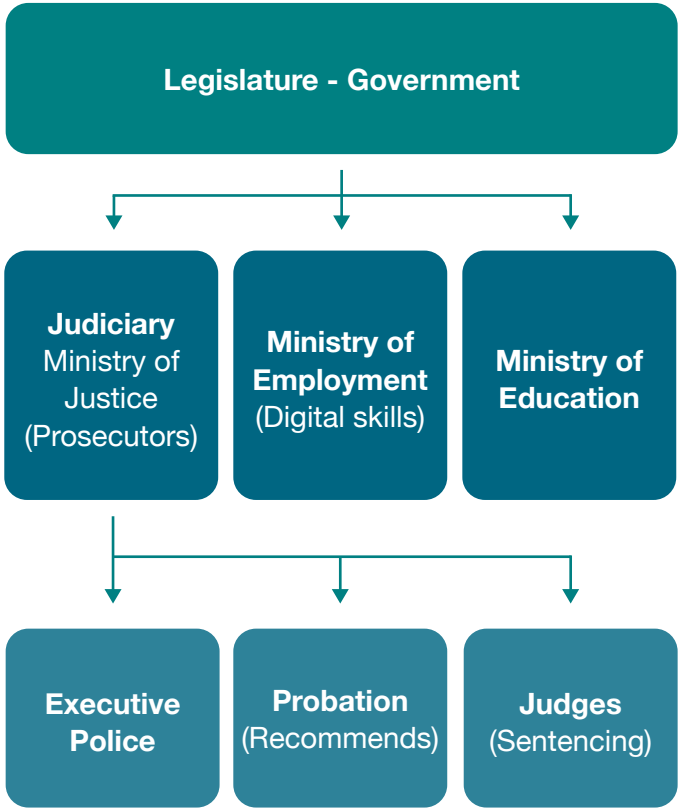


Figure 9: Cybercrime prevention macro strategy - legislature, judicial, executive (Copyright 4D Cyber Security

In support of a National Cyber Security Policy, a working group should be established, meeting on a regular (quarterly) basis with stakeholders to assess, assist and direct the cybercrime prevention strategy as it evolves and develops policy.

A government representative should be appointed to coordinate implementation of the prevention programme.

Representatives from strategic and operational arms of government described below would also attend these working group meetings.

This process ensures strategy objectives are being worked towards through policies, protocols and procedures. It provides those individuals and institutions tasked with developing and progressing Cybercrime Prevention clarity about their obligations and contributions.

Cybercrime Prevention Working Group:
Government representative (Chairperson).

Core Representative:
Ministry of Justice (Courts/Probation/ Prosecutors).

Police (Police Cybercrime lead, National Prevent Officer).

Ministry of Education (Schools, Colleges, Universities).

Ministry of Technology (Digital industry and skills development).

Satellites:
Ministry for Industry (Banks, Gaming)

Ministry of Communication (Media, Publicity, Promotions).

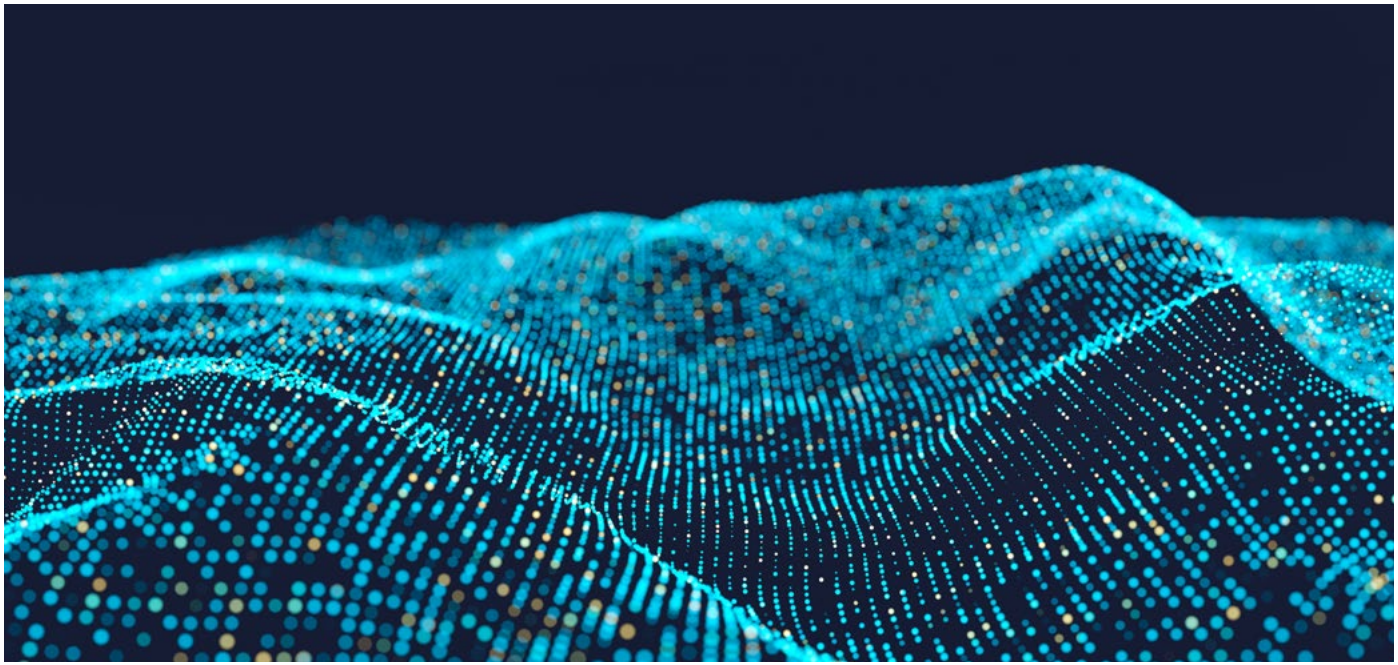
8.0 Cybercrime Prevention National Structure:

8.1 Legislature: Government - National Cyber Security Strategy (NCSS)

The working group should set agreed targets for implementation, progression and completion, providing transparency and accountability for all concerned. The NCSS and working group provide a mandate - and clear direction - for police and Prevent Officers tasked with turning government policy into practical policing.

While this is a government working group, relevant private sector organisations should be consulted as their support later in the process is important. Early involvement from the private sector will instil a much greater level of ownership and empathy.

Cybercrime prevention strategy now moves from central government into the respective ministries to develop and deliver. This is undertaken in a two-pronged approach: judicial and departmental.



"In support of a National Cyber Security Policy, a working group should be established, meeting on a regular (quarterly) basis with stakeholders to assess, assist and direct the cybercrime prevention strategy as it evolves and develops policy."

8.0 Cybercrime Prevention National Structure:

8.2 Judicial – Ministry of Justice

To execute its role of protecting the public, punishing perpetrators and preventing re-offending through tailored rehabilitation programmes, all arms of the criminal justice system will require a joined-up approach to the correct disposal for those found (or pleading) guilty to certain cybercrime offenders.

Where offending is primarily cyber-dependent and certain mitigating factors are present, such as being a juvenile, a first offender, admitting guilt or showing penitence, then a Prevent intervention can be considered part of the criminal justice disposal.

8.2.1 Money or Malice

It is reasonable to characterise the prime motivators for crime - particularly serious crime - as being directly or indirectly related to money or malice. Criminal legislation, offences and respective judicial redress for criminal acts reflect these factors. Aggravating and mitigating factors are always considered, but that does not offset the root stimuli for offending being related to these two motivators.

Profiles of subjects detailed within defence submissions, alongside academic research, offender debriefs and Prevent interventions, such as **Hack_Right** (NL) and Cease and Desist (UK), have identified compelling insights into the motivations of those in the Prevent target audience.

As the industry is so fast moving, gathering insights needs to continue and results shared more widely. Many committed serious cybercriminals have been subject to arrest by national law enforcement.

As documented earlier, those on this Cybercriminal Career Pathway had a marked absence of conventional criminal motivation. Money and/or malice were often absent or secondary to mischief and misunderstanding, although as stated this position may change over time.

This is a consideration that must be explored and understood when formulating judicial policy.

8.2.2 Adjudicators

To attain and retain public confidence in judicial sentencing, options available to judges and magistrates must be tailored to the nature of the individual's offence. The sentence should be fair, just and reasonable. It should punish or the offence and build in provisions to offset re-offending.

Where motivations for cyber offending are fundamentally:

Mischief - through testing digital skills, curiosity and reputational enhancement, or

Misunderstanding - through lack of awareness and understanding of the full legal and life implications of their online- deviance, adjudicators would have prevent community sentencing options at their disposal.

This will provide opportunities for a judge to deter an individual from re-offending. Such sentencing options can also divert offenders towards more legitimate use of their skills, using prevent interventions such as **Hack_Right** or debriefing sessions. Another option might be to simply direct probation to arrange, when appropriate, engagement with the local prevent network.

8.0 Cybercrime Prevention National Structure:

8.2 Judicial – Ministry of Justice

8.2.3 Probation/Youth Service

Probation is a court-ordered period of offender supervision as an alternative to serving time in prison. All countries considered under the CMAGE model have Probation as a functional service, or in their statutes as an option for sentencing.

In some jurisdictions, probation applies only to community sentences such as suspended sentences. In others, it can include supervision of those conditionally released from prison on parole. How probation fits within the respective criminal justice systems is key to the prevention of cybercrime.

Probation Services (Bangladesh) summarises its function as follows: "The purposes of probation are the prevention of offences and recidivism as well as fostering rehabilitation, reintegration, non-stigmatization of offenders, and, in some cases, restitution to the victims."

Taking this version as the template, prevent community sentencing options fit perfectly in the criminal justice systems of the CMAGE-analysed countries.

This enables a Probation Officer, when reviewing an offender's circumstances, to consider proposing to the court bespoke community sentencing options that can involve Prevent Officers.

A Prevent Officer can be recommended to help probation steer the individual towards an appropriate intervention. This joined-up approach brings the system full circle from police to prosecution to adjudication (sentencing) to probation to police (Prevent Officer).

The offence may be so serious that the individual is imprisoned, but that does detract from the fact that probation can be utilised with a Prevent intervention after incarceration.

"The purposes of probation are the prevention of offences and recidivism as well as fostering rehabilitation, reintegration, non-stigmatization of offenders, and, in some cases, restitution to the victims."

8.0 Cybercrime Prevention National Structure:

8.3 Cybercrime Prevention Officer/Prevent Network

The Prevent Officer's role is explained in full throughout this guide, so specific detail is not required in this chapter. Suffice to say the need for law enforcement to provide services that support the judiciary, post sentencing, is seldom actively prioritised.

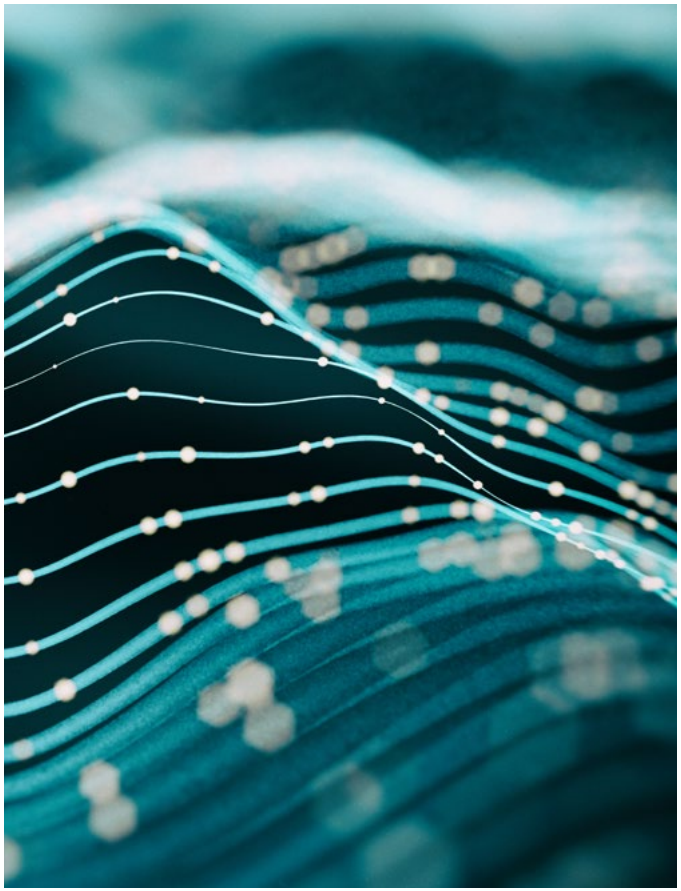
In revisiting the principles of policing and the premise that its primary role is to "prevent crime and disorder", it makes perfect sense for police to play a role in keeping individuals from offending - and if that fails, help keep them from re-offending.

The Prevent Officer, through regular briefings on operational matters, may identify an individual who might be receptive to a Prevent intervention. The Prevent Officer would at no stage interfere with the wheels of the criminal justice system until the individual comes out the other end. Only after the judicial disposal, (whether no further action, a community sentence or imprisonment is declared), would a Prevent Officer become involved.

This is a key determinant of Prevent engagement. The Prevent Officer role is not to become involved in review and assessment of a convicted person pre-sentencing as this could be seen as preferential treatment for the offender. It could also be interpreted as a mechanism for influencing criminal justice outcomes though Prevent Officer advocacy by lawyers and others.

If it transpires that the judge deems a community sentence appropriate, then it is appropriate for the Prevent Officer to become directly involved as per the court order, or engaged via the Probation Service, depending on the respective judicial process and resources available in the country.

"The Prevent Officer, through regular briefings on operational matters, may identify an individual who might be receptive individual comes out the other end."



8.0 Cybercrime Prevention National Structure:

8.4 Departmental - Ministry of Education

Law enforcement, criminal justice systems and the cyber security industry are aware of the increasing number of young people becoming involved in cybercrime. Very few others are. As bold as this statement is, it rings true in too many countries.

Education departments, together with private sector partners can help raise awareness of:

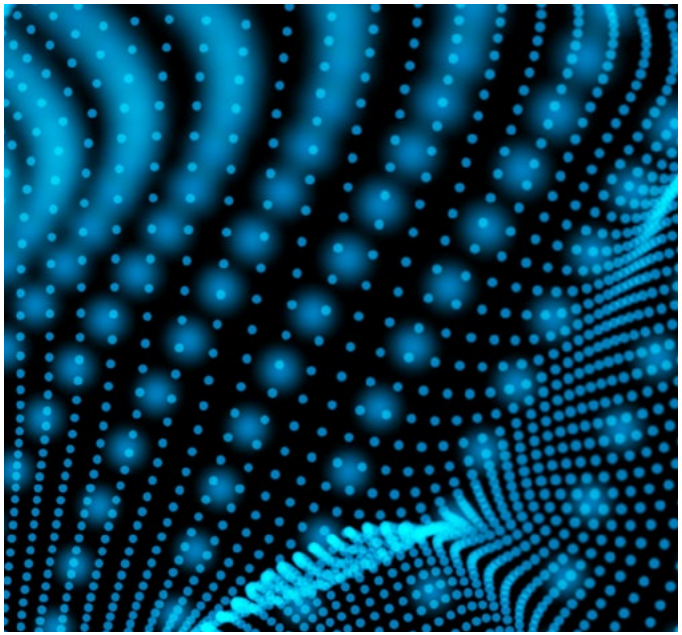
- Routes into cybercrime
- Legal and life implications of cybercrime
- The importance of online social responsibility
- Legitimate opportunities for those with interest or skills in digital technology

Through communication campaigns and on- and offline learning resources, education departments can facilitate the development of relevant skills necessary for avoiding being drawn into cybercrime.

Key skills include:

- Structured decision making
- Risk assessment
- Understanding of criminal pathways
- Ability to recognise manipulative techniques
- Effective use of exit strategies, while providing key facts about cybercrime

At the heart of the education remit is the aim of ensuring anybody who becomes involved in cybercrime at any age, from any background, in any demographic, has made an informed choice. If an individual comes to the attention of law enforcement by cyber offending, they should be fully aware of the above list of points and have consciously chosen criminal activities. This awareness can be developed by ensuring digital skills education (particularly coding) builds in understanding of the legislation that guides "unauthorised access" and related computer misuse offences. In simple terms, you can't teach someone to be a locksmith without teaching them the legislation regarding use of their skills - such as trespass, theft and burglary.



8.0 Cybercrime Prevention National Structure:

8.4 Departmental - Ministry of Education

Education departments should dictate that digital skills tuition must include cybercrime legislation and online social responsibility. This could be developed into a module on Cybercrime Prevention. There is fortunately no need to 'reinvent the wheel'.

The UK's NCA has developed a comprehensive package of **Learning Resources**, including presentations and videos to assist teachers with cybercrime prevention lessons. (PSHE, 2020).

- What cyber enabled and cyber dependent mean
- Causes and potential pathways into cybercrime
- The impact on victims and negative consequences on individuals of cybercrime
- How to avoid harmful influences online
- Opportunities, via formal and informal education, in employment in digital industry and associated sectors

The lessons are comprehensive, delivered in plain English, with an option for subtitles to be added. Jenny Fox from the PSHE Association states: "These lessons provide the background knowledge needed to deliver high quality teaching and learning about the risks of cybercrime.

As our lives increasingly involve technology, young people need opportunities to develop skills and understanding to navigate the online world, including in relation to the law.

Through an engaging case study, students are able to evaluate the real-life consequences of decisions made online."

It is important to stress the target audience is not prescriptive. Although aimed primarily at students, the lessons are just as important and effective for informing parents, guardians and society at large.

Society in greater numbers is impacted by cybercrime, but largely ignorant of its seemingly complex dynamic.

"Education departments should dictate that digital skills tuition must include cybercrime legislation and online social responsibility. This could be developed into a module on Cybercrime Prevention. There is fortunately no need to 'reinvent the wheel."

8.0 Cybercrime Prevention National Structure:

8.5 Ministry of Employment/Skills (National Development)

Africa and Asia, like the rest of the world, currently face a significant digital skills gap. With a growing population, this gap will only widen in future - unless significant measures are taken to fill it.

The International Finance Corporation (IFC), a World bank affiliate, stated in 2020, “Africa faces a huge digital skills gap, which is diluting economic opportunities and development. Some 230 million jobs across the continent will require some level of digital skills by 2030.”

The IFC estimates: “potential for 650 million training opportunities and an estimated US$130 billion market. With the COVID-19 pandemic forcing many businesses to go digital to survive, the need for these skills has only become more apparent in recent months.” (Caballero and Bashir, 2020).

One Asian country consolidates this view of a panoramic digital skills shortage. The World Bank, in reference to one country in the CMAGE regions, projects “a shortage of nine million skilled and semi-skilled ICT workers by 2030”. The World Bank suggests this figure is indicative of many other countries but added that it has “started programs to address digital infrastructure requirements, human resources capability… improving skills of workers, creating jobs in technology-based entrepreneurship and revamping of vocational education institutions.” (The World Bank, 2018).

There are initiatives across the Africa and Asia regions to develop in-country digital capability. Clear examples of the dearth in digital skills have seen several public/private sector initiatives delivering training and job opportunities for the technology sector.

The promotion of these opportunities through the respective ministry will provide the Prevent Network with a purposeful, practical and attractive tool when messaging and interacting with key target audiences, particularly parents and children.

There is no better stimulus for a parent or guardian than a child’s career choice that provides immediate employability after qualification with a competitive salary. For young people enlightened about the marketability of their digital knowledge and skills in the legitimate world, they obtain an enhanced sense of value and self-esteem.

Cybercrime prevention connectivity to digital skills initiatives - advocated and led by a Ministry of Employment/Skills - directs potential and incidental cyber offenders away from overstretched criminal justice systems and towards needy industries where their technical skills can be productively employed.

Digital skills initiatives lead by a Ministry of Employment or Skills helps drive cyber offenders into worthwhile careers where their skills are not only valued, but desperately needed.

Such cybercrime prevention activities also help alleviate some of the issues overstretched criminal justice systems face.

Government-led digital human resource initiatives provide patriotic investment platforms for national development and future-proof the ever-growing digital technology sector.

8.0 Cybercrime Prevention National Structure:

8.6 Executive: Police

The police, as an executive arm of government, will be at the forefront in delivering Prevent objectives laid out in any government cyber security strategy. They will be the public-facing medium for Prevent. Through the Prevent Officer and Prevent Network, the public will be able to access cybercrime prevention resources.

The illustration to the right provides an indicative structure for implementation management and coordination of cybercrime prevention through the police.

Armed with a directive from the legislature (government), a police national cybercrime unit would appoint two Prevent Officers.

Those officers will have clearly delineated roles: ***Strategic*** and ***Operational***.

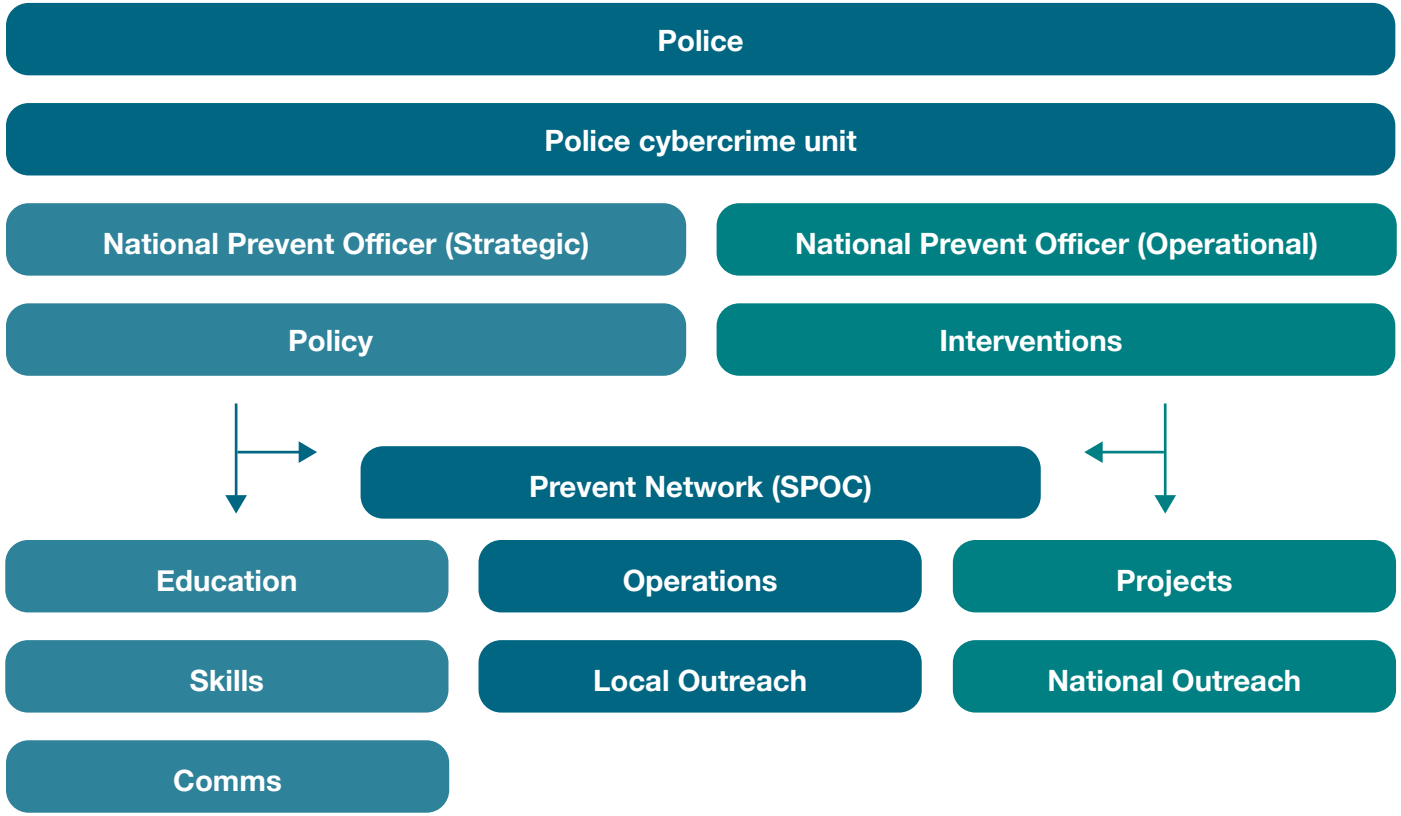


Figure 10: Indicative structure for the implementation management and coordination of cybercrime prevention through the executive branch of government, the police. (Copyright 4D Cyber Security Ltd)

9.0 Prevent Officer - Strategic

Introduction

The Cybercrime Prevention Officer holding the strategic portfolio will be responsible for structural elements of the legislative directive. They will work with the Ministries for Justice, Education and Employment to ensure Prevent requirements are met, as directed by the government.

They will be expected to meet with representatives from the Ministry of Justice including probation, adjudicators, prosecutors and youth offending teams (social services) to ensure Prevent lands properly within their field of operation, policy and procedure.

9.1 Working Groups (WG) - Ministry of Justice

Working groups should be established with representatives from the respective areas outlined, meeting regularly to determine ownership of issues and implementation of actions. This will ensure government macro prevent strategy is weaved into the fabric of the ministries required to meet the objectives, mechanisms for implementation and action required.

9.2 Working Groups (WG) - Ministry of Education and Employment (Skills)

This WG, comprising Ministry of Education and Employment representatives, would work in tandem to ensure they cross fertilise each other.

The educational remit helps raise public awareness of Prevent by providing access to educational modules. Teachers, community leaders and parents will be able to deliver these modules and tailor them for in-house presentations for institutions and businesses. By ensuring cybercrime prevention is a component part of the development of young people in an interconnected world, you begin to normalise behaviours and practices that were previously ignored, misunderstood or misrepresented.

The employment remit would publicise and promote digital sector opportunities and identify and secure private sector partners to sponsor or co-sponsor initiatives that develop the right skills.

It is important that the employment opportunities for the wider digital sector is included, as not everyone identified will want or have the opportunity to enter the cyber security industry.

This public/private coalition is central to Prevent and explained in depth within this guidance.

Suffice to say, a measure of success for Prevent will be individuals that can be evidenced as being deterred and diverted from cybercrime into careers involving the same digital interests, skills and abilities.

The Prevent Officer holding the strategy portfolio would either exclusively, or with their operational colleagues, attend these meetings - and where necessary, coordinate meetings between representatives from all the ministries.

A senior police representative and the coordinating government civil servant would be expected to attend some working groups and be briefed on Prevent objectives' progress by the respective ministries.

The Prevent Officer will be expected to identify procedural or departmental blockages and expedite matters.

9.0 Prevent Officer - Strategic

9.3 Communications

Communications campaigns will be managed under strategy. The Prevent Officer will be responsible for determining the target audience for online and offline material including leaflets, brochures, news articles and videos.

Examples that can be replicated, and in the case of videos used free of charge, include:

- Cyber Choices
- A Hack Too Far

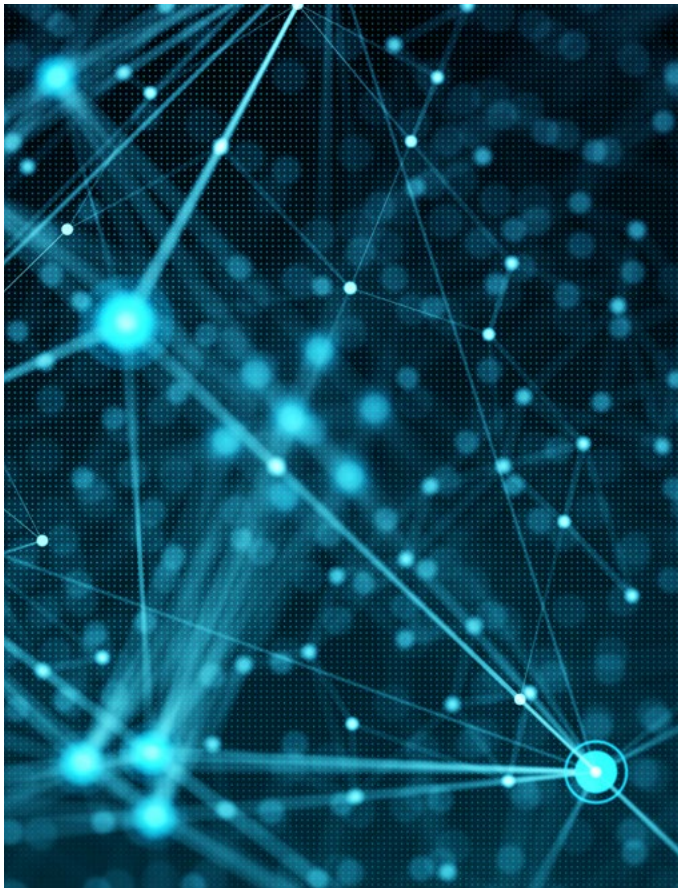
This is an area where partnership with companies (private sector organisations who will obtain direct benefit from a Prevent campaign) is paramount to securing external funding and for sharing responsibility in addressing issues. The gaming industry can be an excellent ally. They suffer more Denial-of-Service attacks than any other industry and aspects of their landscape - namely 'modding' and cheating - have been identified as a gateway for some into cybercrime.

Gaming: The NCA Prevent team has been attending the most high-profile gaming events in the UK since 2016. It hosts an exhibition stand and provides information, technical challenges and demonstrations such as ethical hacking.

The activity enables prevent officers to engage directly with their target audience and those responsible for them, parents, teachers and guardians. The Cyberchoices stand is incredibly well attended
and championed by the gaming companies at the events.

Other tangible support for Prevent campaigns is evidenced in the Netherlands where the Cyber Offender Prevention Squad (COPS), police and gaming sector representatives work with public and private industry to stimulate youngsters' interest in the legitimate use of their digital skills and abilities (**see appendix 1, Politie.nl, 2021**).

"The NCA Prevent team has been attending the most high-profile gaming events in the UK since 2016."



9.0 Prevent Officer - Strategic

9.4 Research

During the last five years, a growing body of academics have provided insightful research into the human aspects of cybercrime, significantly benefiting cybercrime prevention. Research has been undertaken both in collaboration with, and independent of, the various arms of cybercrime prevention.

Areas of interest include studies on Youth Pathways into Cybercrime (NCA/Europol); the effectiveness of law enforcement cyber operations (Cambridge University), and Modelling online criminal networks (Professor David Wall).

The Prevent Officer would work with academia to shine light on nuances and areas of mutual interest in their respective Prevent landscape. Findings from established academic institutions can provide additional evidence to support and if necessary, redirect, prevent initiatives and interventions.

9.5 Child Exploitation and Online Protection (CEOP)

In the UK, CEOP is tasked to work both nationally and internationally to bring online child sex offenders to court. Like its cybercrime prevention counterparts in the National Crime Agency, CEOP combines police powers with expertise from the business sector, government, specialist charities and other interested organisations to develop and implement initiatives and interventions that bring online child sex offenders to justice.

CEOP's experience, particularly its Virtual Global Taskforce (VGT), could assist with securing buy-in to, and sponsorship of, cybercrime prevention and assist with tailoring representations to key stakeholders.

The VGT has built an effective international partnership of law enforcement agencies, non-government organisations and industry to help protect children from all forms of online child abuse.

The Strategy Prevent Officer has a demanding role in one of the most stimulating areas of cybercrime. They must work in tandem with their Operational Prevent counterpart to ensure their respective portfolios are joined up and focussed on achieving the national cyber security strategy, alongside other actors in the public and private sector.

"Findings from established academic institutions can provide additional evidence to support and if necessary, redirect, prevent initiatives and interventions."

10.0 Prevent Officer - Operational

Introduction

The Operational Prevent Officer will be primarily responsible for the following areas:

- Identification and implementation of prevent-led operations, coordination of initiatives that support and/or amplify operational team activities
- Recruitment, development and management of the single points of contact (SPOCs) that form the prevent network, and
- Developing and delivering in-country prevent interventions through the prevent network and local partners

10.1 Operations

This Prevent Officer must keep abreast of all Operations to ensure opportunities for Prevent interventions (on- or offline) are built into the plan from the earliest stage. This proactive approach connects and consolidates Prevent rationale with the traditional operational arms of the Police and provides opportunity for full use of the 4D approach: Deter, Divert, Degrade, Disrupt.

All international operations with a Prevent component will be coordinated through this arm of Prevent, ensuring where practical, that Prevent activity impacts on criminal actors causing harm to the respective country from another country.

10.2 Interventions

The Prevent Officer must ensure the correct interventions are identified for operational work and deployment through the Single Point of Contact (SPOC) network.

Acting on feedback from the Prevent SPOC Network, Prevent Officers will review and assess the functionality of interventions and make representations to the Strategic Prevent Officer for amendments to policies, protocols and processes.

10.3 Projects

There will be a requirement to review ideas for new interventions that emanate from the Prevent Network and partners and where practical, initiate working groups to formulate and progress projects.

10.0 Prevent Officer - Operational

10.4 National Outreach

The Operational Prevent Officer will work with the Strategic Prevent Officer to source and solidify contacts with the private and public sector which can progress the cybercrime prevention strategy.

"The Operational Prevent Officer will direct the Prevent network in conducting "Cease and Desists" and positive diversion workshops, alongside intelligence development and deconfliction."

They will help identify individuals and initiate communication, nationally and regionally, with the digital industry, financial sector and academia who can work with the Prevent Network.

The aim is to secure ancillary funding, services and resources. This would include establishing and facilitating coding and technology clubs. This resource is explained elsewhere in this guidance.

10.5 Prevent SPOC (Single Point of Contact) Network

The Prevent SPOC Network will be formulated through an "expression of interest" campaign to police officers, coordinated by the Prevent Officer who will ensure understanding of, and connectivity to, the strategic strand.

The Operational Prevent Officer will direct the Prevent network in conducting "Cease and Desists" and positive diversion workshops, alongside intelligence development and deconfliction.

They will hold regular forums for exchange of information, ideas and issues and arrange a national conference with their strategic partner.

The training and upskilling of the Prevent Network will be central to this role, ensuring the Prevent SPOCs are prepared for execution of their duties and subject to continued professional development (CPD).

10.0 Prevent Officer - Operational

10.6 International Prevent SPOC Network

For Prevent to maximise its impact domestically, it must have connectivity with the rest of the world. Country-specific prevent activities can achieve excellent, but limited, results – especially if those attacking a particular country are outside of the jurisdiction and/or scope of influence.

This guide proposes that each country under CMAGE would have a Prevent Single Point of Contact (SPOC). Collectively, they would form an international network of Prevent SPOCs. The network would cross-fertilise support, experience and contacts to develop and implement their respective Prevent programme. Cybercrime operations across the network would be enhanced by coordinated Prevent activity within the source country and across the region. Such coordinated activity increases the perception of risk of law enforcement intervention.

By raising the awareness of Prevent tools and techniques to all countries in the African and Asian regions, and sharing good practice, the CMAGE Prevent SPOC Network can build an increased risk awareness and action against those both peripheral to, and immersed in, cybercrime. This will help offset criminal traffic attacking the region and provide a joined-up global approach to addressing cybercrime. Such an approach pulls both the public and private sector into the fight. It awakens all to the reality that if they understand the problem, they can use their combined resources to help offset it.

10.6.1 SPOC Aims and Objectives

i To establish an international joined-up approach to cyber-dependent crime that impacts on both entry-level and high-end cyber enabled and dependent criminals

ii Raising the perception of law enforcement intervention online in as many countries as possible

iii Increasing public/private awareness of cyber-dependent crime and their role in deterring, diverting and disrupting

iv Raising the profile of the Prevent Network and individual country initiatives as being at the vanguard of innovative, impactful law enforcement techniques

This Prevent SPOC Network would lean heavily on the experience of the UK's Child Exploitation and Online Protection (CEOP), particularly the Virtual Global Taskforce (VGT). The VGT has built an effective international partnership of law enforcement agencies, non-government organisations and industry to help protect children from all forms of online child abuse.

11.0 National Cybercrime Prevention Implementation Strategy

Introduction

In this chapter, a plan is outlined for implementing a cybercrime prevention programme to the eight countries cited in this guidance. However, the plan is sufficiently generic to be universally applicable.

An implementation plan should include the following:

Scoping and Discovery - to understand what work has already been undertaken within each country and to enable country -specific scopes and plans to be developed.

Detailed Design - to specify and summarise the people, processes and system recommendations required to deploy the 4D Prevention model and supporting ways of working.

Adaptation and Change - to lead the change efforts within governments, criminal justice systems and private and public sectors through a coordinated, collaborative, implementation approach. This will inform, educate, adapt behaviours and raise awareness of the new Prevent model and increase capabilities to support country deployment.

For a programme of this scale, monthly steering group discussions would be required. Based on the strategy described, a Prevent Implementation Model has been drafted on the following page.

11.0 National Cybercrime Prevention Implementation Strategy

Introduction

CREST CMAGE Project Management (CPPM)

Prevent Implementation Team (PIT)

4D Cyber security (4DCS) Consultancy

Country One | Country Two | Country Three

Monthly

- Champion the Prevent Programme across the country artculting the benefits and opportunities
- Resolve challenges and clear major risks and issues
- Ensure stakeholders are engaged throughout the programme and that communication is effectively managed
- Track progress of key milestones against the project plan
- Understand alignment of project deliverables across the countries
- Create monthly status report, showing progress, decision requirements and next steps

Meetings with Africa/Asia prevent SPOC's

Country One | Country Two | Country Three

Weekly

- Meet with the Prevent SPOC's weekly to discuss upcoming activities and then execute prevent activities.

Programme team to discuss:

- Overall Red Amber Green (RAG) status
- Milestone status
- Key achievements
- Risk, issues and net steps

Prevent implementation Team Meetings (PIT)

Prevent Implementation Team (PIT)

Core Prevent Team
Weekly Drum Beat
Start of Week Work Stream Review

Weekly

- Resolve challenges and clear major risks and issues
- Ensure relevant members are engaged and that communication is effectively managed
- Track progress of key milestones against the project plan
- Track benefits in line with the business case
- Weekly status reports will be consolidated on a weekly basis

Figure 11: Prevent Implementation Model (PIM)

11.0 National Cybercrime Prevention Implementation Strategy

11.1 Phase One - Scoping exercise

A comprehensive review of the Prevent landscape for each country is required.

This would include:

- National cyber security strategy or equivalent (legislation, policy, budget)
- Nature of cyber-attacks (cyber-enabled, cyber-dependent)
- Volume of cyber-attacks
- Source of cyber-attacks (demographic, domestic, international)
- Socio-economic impact of cybercrime (harm to country)
- Private sector technology profile (partnership/sponsorship)
- Public sector technology profile (partnership/communication)
- Law enforcement cyber capability (resources/equipment)

11.2 Phase two: Recruitment, Advocacy, Planning

11.2.1 Recruitment

Recruitment of the National Strategic and Operational Prevent officers (see appendix 2 and 3 for profiles) in each country would be prioritised to create an African-Asian Prevent Network. These individuals would act as the single point of contact (SPOC) for Prevent in their respective country. They would work independently and collectively to develop Prevent in their country as outlined in the strategy model with the Project Implementation Team.

11.2.2 Advocacy

This stage requires a comprehensive consultative initiative with key stakeholders in the private and public sector. By identifying and convincing key personnel in government and business, advocates are created who can promote the Cybercrime Prevent rationale and impress the “low resource, high impact” model for implementation. Representatives from the public and private sectors would also liaise with the Project Implementation Team (PIT), the project champion, and if necessary CREST CMAGE Project Management (CCPM).

11.2.3 Planning

This phase requires determining the “best fit” Prevent interventions based on the in-country scoping outcomes from phase one. Ideally, the Project Implementation Team (PIT), would work with the Prevent Network to identify an online and offline intervention to showcase the “low resource, high impact” of prevent activities, virtually and in the real world. Academia would be a component part of this phase, sourced by the PIT. Academic input will help determine the best measurement tools for interventions and provide empirical evidence for determining the efficacy of the Prevent programme.

11.3 Implementation

Once the preparatory work is undertaken, the interventions in place and effective dates determined, the initiative should be launched. The Prevent Implementation Team should create a bespoke communications plan to amplify the activity online and offline. Metrics for measuring the impact of the campaigns will be established and monitored, and results escalated to the Crest CMAGE Project Management (CCPM) for dissemination, as appropriate, to primary stakeholders.

Metrics and Measurements

- 12.0 Prevent Model
  - *12.1 Impact Supersedes Volume*
  - *12.2 Academic Validation*
  - *12.3 Cease and Desist Visits: Recidivism*
  - *12.4 Hack_right*
  - *12.5 Positive Diversion Workshop*
  - *12.6 Degrade/Disrupt: Warning Emails*

12.0 Metrics and Measurements

Introduction

Modern day policing is (justifiably) heavily focused on performance indicators that measure success and failure by factors including the number of arrests made and offences committed. However, the following two areas of offending stand aside from conventional metrics: terrorism and cyber-dependent crime (CDC).

With terrorism, an individual or group can impact national psyche through the indiscriminate, violent nature of their attack; hence significant resources are given to counter terrorism (CT). CT by its nature, is Prevention.

Success in CT activity is measured by number of plots detected, individuals arrested and absence of attacks. As referenced earlier, Sir Robert Peel laid out nine principles for modern policing.

The following principle resonates directly with measurements for cybercrime prevention programmes: “Whether the police are effective is not measured on the number of arrests, but on the lack of crime.” (Lentz and Chaires, 2007).

12.1 Impact Supersedes Volume

Cyber-Dependent Crime should arguably be measured in the same way. An individual or group can cause immeasurable damage to institutions and the social fabric through targeted attacks against key digital infrastructure. They can, and have, caused national security issues.

The impact and damage can be so serious that it warrants national and international intelligence service and law enforcement intervention.

By assessing cyber-dependent crime through its capacity for one individual or group to cause significant damage, it is clear that **impact supersedes volume**. Using the ‘Impact over Volume’ metric cemented the rationale for investing in a comprehensive cybercrime prevention programme in both the UK and the Netherlands. Bespoke cybercrime prevention activity can demonstrate effectiveness in reducing cybercrime over a protracted period. The ‘online adword’ campaign conducted by the UK Prevent Team is a perfect example. In January 2018, the first month of the campaign, keyword searches by a target group of 12-24-year-old are displayed in the following table.

	January 2018 (30 days)	September 2019 (30 days)
Click-throughs (Link to NCA Prevent website was used)	500	170,000
Impressions (Warning Notifications)	13,000	1,900,000

Figure 12: Adword (Google Ads) campaign aproximate statistics

Tailoring the ‘AdWords’ to school holidays and high profile, youth orientated, on- and offline events with targeted media reporting, led to the significant increase displayed in the above table for September 2019. Although approximated, the rise of click-throughs and impressions is valid. The campaign also built-in operational activity being conducted by domestic and international law enforcement agencies with particular emphasis on the take-down of infrastructure and arrest of individuals involved in providing Denial of Service capability to whoever would pay.

12.0 Metrics and Measurements

12.2 Academic validation

In 2019, Cambridge University released a research paper outlining the effectiveness of law enforcement interventions against Denial of Service (DDoS) attacks. They assessed the effectiveness of primarily domestic and global arrests; "booter" website take-downs and messaging campaigns (UK Adwords).

Regarding the volume of DDOS attacks, the researchers observed: "In the US, France, Germany, Netherlands, Russia, and Poland, we observe a continuing upward trend from the beginning of 2017 up to the Webstresser take-down in April 2018. In the UK, however, this upward trend flattened off entirely from December 2017 until June 2018. This flat trend continues until August, whereupon there was a large spike in attacks and the series begins to grow again." (Collier et al, 2019).

Cambridge University was strident in its findings, stating: "We believe the adverts have led to a clear and lasting reduction in the number of attacks." (Collier et.al, 2019). The paper also suggests the 'Adword' campaign dissuaded users from becoming involved, thereby halting the rising demand for attacks in the UK. The 'Adword' campaign concept is now both integral to UK and Dutch Cyber Prevention interventions. It is considered one of the most progressive interventions devised and implemented by digital law enforcement globally, and a classic example of "low resource, high impact."

Cambridge University's research provides empirical evidence that in the absence of an effective and informed Prevention programme, the volume of certain cyber-attacks increases.

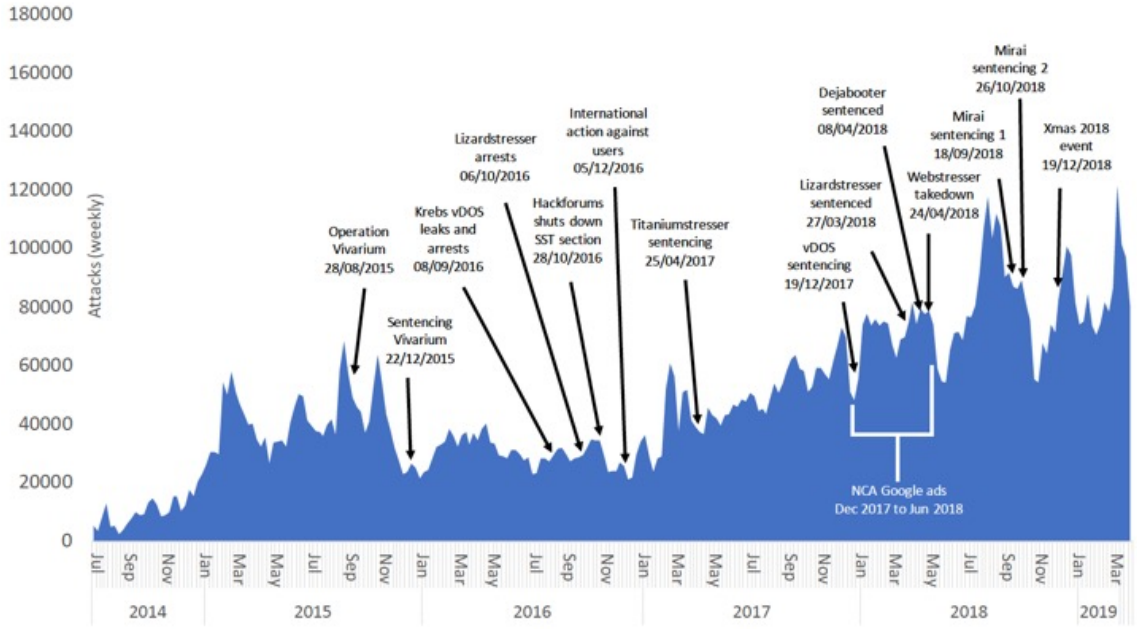


Figure 13: Timeline of intervention events and the number of reflected UDP DoS attacks per week (Collier et.al., 2019)

12.3 Cease and Desist visits: Recidivism (re-offending)

Recidivism or re-offending is the repetitive pattern of: arrest – prosecution – punishment – release – arrest – prosecution.
"For the year ending March 2018, the UK re-offending rate for children and young people (the percentage of offenders who re offended), was 38.4%." (UK Youth Justice Board, 2019)

Anecdotal evidence from the UK Prevent network indicates a low re-offending rate for those who have received a 'Cease and Desist' visit. Approximately 500 cease and desist visits have been conducted since 2012. There have been no more than two individuals come to the attention of the police after the intervention. Even if this figure increased, it is likely that the percentage of recidivists would be considerably less than those committing traditional offline crimes. This is unquestionably a credible advertisement for cybercrime prevention if validated empirically.

At the time of writing, research is being undertaken by a prominent university to study the effectiveness of 'Cease and Desist' and other cyber prevention initiatives. Nevertheless, the initial evaluation is of value for this guidance.

12.4 Hack_Right

The Dutch **Hack_Right** programme that educates and mentors young people convicted of cyber-dependent crime offences has not seen any attendees of the programme back in the frame for the same or similar offences.

12.5 Positive Diversion Workshop

The same can be said for Positive Diversion Workshops. Since 2016, nine workshops have been conducted, with approximately 100 people attending. There are no published reports of any attendees returning to their past behaviour.

Figure 14: Image of Positive Diversion Workshop attendees (BBC Hacker Bootcamp, 2016)

Anecdotal reports from the Prevent Network indicate a less than 5% regression back into cybercrime. The feedback below is from BBC Click, the global technology TV show that featured the first NCA "bootcamp" for hackers.

One of the attendees, a 15-year-old excluded from school and a prolific cyber offender, made a statement underlining why these interventions are deemed successful: "I found that my true passion was actually stopping these attacks from happening. That's how I now get my enjoyment. I have learned what I can do, what course I can take and how I can proceed into cyber security." (BBC News, 2017).

> *"I found that my true passion was actually stopping these attacks from happening."*

12.0 Metrics and Measurements

12.6 Degrade/Disrupt: Warning Emails

This intervention has been utilised on at least two occasions to degrade and disrupt. On separate occasions, approximately 10,000 and 7,000 individuals were targeted with warning emails, referencing their nicknames and the operation. They were advised to 'cease and desist' from their online criminal interest or activity or face further investigation and potentially arrest and prosecution.

The database had been obtained from the take-down and arrest of individuals operating a criminal marketplace. Those emailed were either registered, interacting on, or engaging in, relatively low-level criminality.

On both occasions, responses were minimal and from individuals professing to be researchers or curious observers, asking for no further follow up from law enforcement. The operation was deemed a success simply because there were few complaints from recipients. For the first time, the cyber police had a tangible presence and impact on a criminal community that invariably escaped their attention because of their volume and level of offending.

Due to the sensitivity of 'degrade and disrupt' operations little more can be said about the nature of such interventions and the results. Suffice to say, they are core cybercrime prevention team interventions and are growing in their importance and impact.

Research into the efficacy of cybercrime prevention activities is ongoing with several projects currently underway with the UK Home Office and global universities. The concept is new, and as it evolves more empirical evidence will be produced to help attain and maintain effective interventions and credible mechanisms for measuring results.

That aside, the initiatives and interventions utilised for cybercrime prevention have been deemed so effective by the UK that more than 70 officers are now allocated to this purpose as a nationally managed, locally delivered, Cybercrime Prevention Network. The growth has been practitioner-led.

Cybercrime investigators report back to senior management teams about their observations, and impact of their personal interventions. Their interactions, initiatives and instinct when dealing with target audiences made compelling arguments for more cybercrime prevention.

These officers are now based at regional and local level, centrally coordinated by the NCA's NCCU Prevent Team. They are the public face of cybercrime prevention.

The Prevent Network has a distinct understanding and presence in its localities. This allows it to integrate and pro-actively identify and interact with Prevent target audiences.

The officers can forge local public/private sector partnerships that are committed to addressing prevention issues.

Dedicated Cybercrime Prevention teams in the Netherlands and Finland are now in place, reflecting global interest from nation states for alternative strategies to combating cybercrime, that complement and enhance traditional methods. It is also worth reiterating that some aspects of Prevent work simply cannot be measured in numbers.

Digital Responsibility

- 13.0 Prevent Model
  - *13.1 Self Policing*
  - *13.2 Adolescent Digital Learning vs Adult Analogue Understanding*
  - *13.3 corporate Digital Responsibility*
  - *13.4 Tech and Coding Clubs*
  - *13.5 Your Companies and Country Need You!*
  - *13.6 Cyber Prevention Learning*
  - *13.7 Capitalism with a Conscience*

13.0 Digital Responsibility

Introduction

Gen Z and Millennials are growing up as digital natives with limited understanding, interest or connectivity to the world before computers and associated technologies. The Oxford dictionary defines a digital native as: "A person brought up during the age of digital technology and familiar with the internet from an early age." (Oxford Dictionary, Lexicon, 2021)

The social impact of the cyber eco-system, particularly on our young, has not been fully assessed or understood.

The Cyber Criminal Career Pathway details, among other things, the intoxicating lure of problem-solving, and technical challenges that provide reputational enhancement and kudos.

This dynamic, coupled with largely unregulated personal and digital exploration, can be explosive if it culminates in illegal activity, law enforcement intervention and significant harm to individuals and institutions.

This expansive, loosely regulated, digital landscape can be described as the new 'Wild West'. Cybercrime is increasing, compounded by the Corona-virus pandemic, remote working and increased global digital connectivity.

A 2020 Europol report on cybercrime and COVID-19 states: "...we can trace how criminals have used uncertainty and change to identify and exploit opportunities targeting individual citizens, businesses and the public sector." (Europol, 2020)

"This expansive, loosely regulated, digital landscape can be described as the new 'Wild West'. Cybercrime is increasing, compounded by the Corona-virus pandemic, remote working and increased global digital connectivity."

Cybercrimes' borderless nature, various actors, technical nuances and inconsistent international legislation are additional factors that inhibit effective regulation of cyberspace. Law enforcement does not have the capability to police it.

While domestic and international cyber operations impact on certain markets or activities, evidence suggests the effect is temporary, and only on top tier actors and facilitators.

Entry into cybercrime - and capacity to operate at a certain level without intervention is not difficult.

For those who progress onto more serious offending and provoke the interest of law enforcement, the resources required to investigate, arrest and prosecute are extensive, but significantly compromised if the actor is not in a cooperating jurisdiction, or a juvenile.

13.0 Digital Responsibility

13.1 Self-Policing

Cyber prevention advocates self-policing of all our interactions with digital technology. We, as participants in a global society, must be digitally responsible in terms of compliance with legal, safety and ethical standards. Parenting website, raisingchildren.net.au outlines the key components of being a responsible digital citizen.

It states that all must:

- Have the online social skills to take in online community life in an ethical and respectful way
- Behave lawfully, for example it is a crime to hack, steal, illegally download or cause damage to other people's work, identity or property online
- Protect your privacy and that of others
- Recognise your rights and responsibilities when using digital media
- Think about how your online activities affect yourself, other people you know and the wider online community

Our own moral codes, behaviours and values must be maintained online and reflect the societal checks and balances that govern the real world and contribute to our self-development.

Accounts of those drawn into cyber-dependent crime reflect a marked absence of digital responsibly.

At the most important time of a young person's emotional and social development where self-control can be lacking there is insufficient advice, guidance and regulation of their online interactions.

The issue of low self-control is pertinent. Extensive academic research validates these characteristics and how they can manifest into online deviant behaviour.

Revelock (2019), in a blog, states: "We can recognize a specific phenomenon that relates adolescent criminality to the internet, the impact of low online self-control, which explains why adolescents are more attracted to cybercrimes."

13.0 Digital Responsibility

13.1 Self-Policing

Neutralisation

Over reliance on the internet to justify behaviours that would be frowned on or even be illegal in the offline world. For example, gaining unauthorised access to someone's social media account for 'laughs' is OK, but would not be acceptable if opening someone's letters in the real world.

Anonymity

This concept allows interactions that could be unacceptable if revealed virtually or conducted offline. It provides a cloak of invisibility, that can empower and embolden someone to commit criminal acts. Adolescents believe they are invisible, unidentifiable, which makes them feel more at ease to indulge in criminal activities.

Safety

The volume of low-level criminal behaviour online – such as downloading films, for example, without publicly evident consequences, lowers the perception of risk of punishment for a criminal act.

If a child is interested in the technical aspects of computing such as coding and, programming there are often very few adults in their life that can keep pace with their learning and development. From a cybercrime prevention perspective, normal resources available to parents to progress their child's interest, skills and abilities are too numerous to mention. They might include sports (football, gymnastics etc.) Clubs, dance classes, kumon lessons and music tuition, for example.

Although growing, there is still a paucity of (cyber) resources for young people to immerse themselves in. Ask any adult where their local coding club is, and you will undoubtedly get a vacant look.

13.2 Adolescent Digital Learning vs Adult Analogue Understanding

How can we live in a digital society and not have sufficient resources for technical development that is local, accessible and normalised?

The **2019 Cyber Security report from SANS** (System, Audit, Network, Security) provides a comprehensive assessment of the global skills shortage in cyber security and how young people can help fill the gap.

The report outlines key observations supporting the rationale for a proactive prevention programme, with emphasis on raising awareness and diverting the prevention primary target audience to fulfilling careers.

The report states: "there are concerns around how well-equipped role models - such as teachers and parents - are when it comes to establishing good cyber security hygiene, as well as pointing interested students in the direction of adequate resources to further their interest in the sector." (SANS, 2019).

The value of ongoing public/private sector campaigns promoting digital hygiene cannot be overstated. Education and employment in the digital industry are of even greater value.

Most adults use technology, yet very few understand it. The young use technology, understand it and need, more than ever, to manage and progress it. The world requires the digitally skilled. It is a growth industry, yet there is a dearth of talent in cyber security and related technological disciplines.

"Teen hackers have so much potential and a lot to offer the world of cybersecurity. They're natives to the digital world that they're born into and take to technology like ducks to water. Some of the world's rising stars in cybersecurity are kids and teenagers. It's imperative that parents and teachers alike encourage their curiosity but also teach them to responsibly explore and technologies from a young age." (**Revelock, 2019**).

13.0 Digital Responsibility

13.3 Corporate Digital Responsibility

“Cyber criminals are taking advantage of understaffed and under-resourced companies, who simply don’t have the talent, manpower, budgets and know-how to effectively fend off a bombardment of online attacks…there is no way that the current working population can keep up with the pace of change in cyber security and the widening gap in supply and demand.

There is widespread agreement that the answer lies within our younger generations and more must be done to educate them about cyber security, and the skills needed to protect our digital lives, at a younger age.” (SANS, 2019).

In this context, the concept of digital responsibility - specifically corporate digital responsibility - comes to the fore. All businesses need digitally skilled individuals in a variety of roles.

Careers in cyber security and related fields provide a direct conduit into those individuals who may follow the CCCP.

Business has extensive reach and influence. With the correct focus and communication, business can play a pioneering role in re-shaping society to fit the trajectory of the digital revolution.

It can ensure people are aware of the benefits and detriments of interacting online and provide information and resources for all to contribute positively to society. Corporate investment also gives businesses the opportunity to develop and secure their own pipeline of future digital talent.

“There is widespread agreement that the answer lies within our younger generations and more must be done to educate them about cyber security, and the skills needed to protect our digital lives, at a younger age.” (SANS, 2019).

In this context, the concept of digital responsibility - specifically corporate digital responsibility - comes to the fore.”

13.0 Digital Responsibility

13.4 Tech and Coding Clubs

The importance of digital development resources, on and offline, has been mentioned here previously. Business has a unique opportunity to promote and lead establishment of digital resources such as tech or coding clubs. These clubs can include activities to build awareness of a Cyber Criminal Pathway, relevant legislation, online social responsibility and provide insight into digital opportunities.

Coalitions with academia, law enforcement, Prevent Officers, government departments and charitable organisations can help inform the programme.

Sponsoring businesses can also deliver incentives such as bursaries, work experience, apprenticeships, internships and even employment.

There is no greater stimulant for a parent than the prospect of their child not just developing a skill they love but securing employment from it as well.

These initiatives and incentives are fantastic vehicles for connecting parents to their child's virtual world. They can fully embrace the guidance and stewardship of their child's digital development that they demonstrate in their offline growth and maturity.

The benefits for business are numerous and tangible.

They include:

- Horizon scanning - Investing in the future through the development of a key resource: the new, technically able, socially responsible recruit
- A collaborative approach – this is an example of the sector providing a public service - like steering young people from cybercrime, towards using their skills for good
- Publicity - enhancing their business brand through this activity - i.e., investing in the young and positioning business at the vanguard of "digital responsibility".

"There is no greater stimulant for a parent than the prospect of their child not just developing a skill they love but securing employment from it as well."

13.0 Digital Responsibility

13.5 Your Companies and country needs You!

These benefits can be enhanced with a series of collaborative communication campaigns promoting the steps business is taking to provide "informed choices" for our next generation and to fill the digital skills gap in that respective country. Such campaigns can be coordinated by the Strategic Prevent Officer and actioned by the Operational Prevent Officer and the Prevent Network to include law enforcement, community groups, academia and cyber security professionals.

Many companies are already committed to environmental and social responsibility, seen in corporate-financed community-based projects, often supported through employee volunteering schemes.

Corporate digital responsibility is the next natural, logical step. Financial institutions, banks, tech corporations and others have considerable (cyber, human and technical) resources that could be effectively deployed to support and/or directly deliver a local digital resource. Microsoft is one corporation that has programmes in the CMAGE regions that have integrated digital responsibility as a core business value. Its initiative provides: "*Intermediate-level training to about 500 students via its 'AppFactory' and…250 internships annually… The skills it imparts includes things like how to use professional software for presentations, how to do social media analysis and web design*." (Apolitical, 2019).

A variety of other programmes such as hack the box, the Cyber Security Challenge and coding initiatives such as Africa Code Week are also available for modelling (**see appendix 4, 5 and 6**). There is no need to reinvent the wheel.

13.0 Digital Responsibility

13.6 Cyber Prevention Learning

For direct connectivity to the Cyber Prevention strategy, all learning under the 'digital responsibility' concept should include:

- A module on cyber legislation with real case studies from law enforcement
- A module on online ethics and social responsibility
- Neurodiversity: Its value and impact in the digital world
- Education: Understanding the opportunities for learning and development in the digital world
- Employment: Insight into careers for those showing aptitude for digital technology
- Dynamic delivery: How to devise and deliver a session
- Dealing with classroom issues
- Diversification in the classroom

These fundamentals are to be used to consolidate the ancillary learning provided by the associated business technology team of volunteers who could contribute to sessions and affect change.

13.7 Capitalism with a Conscience

"Capitalism with a conscience" is a mantra widely embraced in the corporate world. Their journeys from environmental to social responsibility, addressing internal and external diversity and confrontation of inequality issues are well documented and prominent in the public domain.

As there is not a business unaffected by the global rise in cybercrime, it makes sense for business to not just focus on cybercrime protection, but to trawl wider, identify future requirements and invest in prevention through commitment to the future – in young, digital natives.

The late Anita Roddick, founder and owner of retail chain, the Body Shop, and one of the leading lights in encouraging businesses to be engines for social change said: "There is no more powerful institution in society than business." (Roddick, 2005).

"Capitalism with a conscience" is a mantra widely embraced in the corporate world."

Conclusion

14.1 Public/Private Partnerships

Cyber Prevention is progressive, proactive, policy making and policing. It has identified a serious problem early by 'horizon scanning' and recognising a rising number of incidents primarily involving technically able young people and their uninhibited relationship with digital technology.

There is also a growing phenomenon of easily accessible and affordable, (if not free), criminal tools available to those interested in obtaining them online.

By building Cybercrime Prevention awareness and interventions into the three arms of government (in collaboration with key private and public sector partners) and exalting legitimate digital opportunities, individuals who may fall into cybercrime are identified early, while talent is preserved and retained.

As detailed in the 'digital responsibility' section, the private sector benefits from those individuals deterred and diverted by law enforcement and their partners. The target audience tends to cease offending and often ends up working in the digital world.

A ZD Net industry magazine article noted: "*It is ironic that while the cybersecurity industry as a whole is generally short-staffed, kids are learning from the sanctity of their bedrooms how to cause utter chaos for enterprise companies with lax security -- and these teenagers may not realize the full impact of their activities, or the potential consequences.*

We need white hat cybersecurity professionals both now and to fulfil future roles, and so giving these kids a chance before their potential is wasted could be a way not only to reduce cybercrime but also to fill the gaps in recruitment."

All those using digital technology, irrespective of age, should be able to make an informed choice about how they interact and engage in cyberspace.

If they enquire about, or undertake, deviant online behaviour, they are subject to the interventions of the 4D approach, that aim to Deter and Divert, if receptive, or Degrade and Disrupt, if resistant.

"By building Cybercrime Prevention awareness and interventions into the three arms of government (in collaboration with key private and public sector partners) and exalting legitimate digital opportunities, individuals who may fall into cybercrime are identified early, while talent is preserved and retained."

Conclusion

14.2 Law Enforcement

Smarter policing, through the promotion of Cybercrime Prevention, must become a reality at all levels of engagement with offenders and all types of cybercrime. However, all the "heavy lifting" cannot be left in the domain of the police, Prevent Officers and their network.

The rationale is that Cybercrime Prevention through the CCCP debriefs and other sources illuminate issues, instigate initiatives and then identify the best individuals or institutions to own and deliver the intervention. For instance, in the UK, the Cybercrime Prevention education modules were collated by the Prevent team and developed and implemented by educational partners.

Police operational teams, through Cyber Prevention, now have an opportunity to deploy a more holistic approach to cyber cases, impacting on the many, not just the few. They can arrest and prosecute the most prolific.

For those at other levels, or outside their jurisdiction they can:

- Raise the perception of risk
- Facilitate informed choices
- Amplify pursue activity
- Reduce mitigation

- Provide effective interventions
- Increase understanding of pathways into cybercrime
- Police to provide service before force
- Deliver proactive policing: horizon scan to anticipate and prevent future serious crimes
- Enhance public perception of the police via all the above

Participant, parent and partner feedback from primarily online advertising campaigns and workshops, but also via 'Cease and Desist' visits, impress the value of police providing "Service before Force."

Law enforcement is tangibly investing time and effort into stopping crime before it evolves, protecting those vulnerable to undue influence and creating opportunities for maintaining healthy digital development. This is healthy publicity for an institution that too often receives very little.

Conclusion

14.3 The Future: Cyber Prevention

It is paramount that Cyber Prevention advocates impress the importance of Impact over Volume. If law enforcement concentrates solely on how many are committing offences as opposed to the capability of the individuals/group and the damage caused, then we will be massively under prepared for increased referrals. This is now being seen online, with uninhibited technical learning without context and the availability of criminal services accessible to more people every day.

Cybercrime Prevention does not profess to stop cybercrime. However, it proclaims, by understanding the human aspects and pathways into cybercrime, that bespoke initiatives and interventions can be implemented alongside conventional law enforcement operations to stem the flow into online deviancy and illegality.

Cybercrime Prevention aims to clear the cybercrime landscape of those there because of lack of awareness and early intervention. Those obligated to provide guidance, advice and regulation of a person's development and interactions in the offline world are being encouraged to replicate the same obligations in the virtual world.

And the earlier the intervention the greater the impact. The further along the pathway, the less effective the impact. Therefore, we must continue with the concept of the courts being involved.

With a good Prevent programme in place, mitigation due to ignorance is less effective. If an individual has already had support from the 'system', the excuse drops away.

This Cybercrime Prevention guidance advocates its necessity and provides a template for its development and implementation.

It offers governments and business a comparatively low resource, high impact investment that has direct benefit to a nation's socio-economic well-being.

It also endeavours to focus government and corporate decision makers on what they want their society's digital futures to look like and how they can collaboratively determine the direction.

In the words of a traditional African proverb given a Cybercrime Prevention, 21st century interpretation:

"It takes a digital village to raise a digitally native child."

"It takes a digital village to raise a digitally native child."

Appendix

- Appendix
  - *Appendix One: Images from Netherlands High Tech Crime Unit encouraging legitimate use of digital skills (Politie.NL, 2021)*
  - *Appendix Two: Cyber Prevention Officer - Strategy*
  - *Appendix Three: Cyber Prevention Officer - Operational*
  - *Appendix Four: Images of the UK's CyberLand Challenge – Cyber Security Challenge/NCA (Cyber Games UK, 2021)*
  - *Appendix Five: Image from SAP Africa Code Week (2021)*
  - *Appendix Six: Overview of Coding Lab Singapore Learning Roadmap (2021)*

Appendix

Appendix 1 – Images from Netherlands High Tech Crime Unit

Appendix 2 – Cyber Prevention Officer - Strategy

EXAMPLE

John Briggs

Cybercrime Unit – Prevent Officer (Strategy)

The Prevent Officer's primary role is to work towards the Cyber Prevention aims and objectives within the National Cyber Security Strategy. They will work with primarily the Ministry of Justice, Ministry of Education and Ministry of Employment to develop mechanisms for progressing the Prevent agenda. They will establish the relevant Prevent working groups and identify the respective civil servants and representatives needed to attend. The Strategic Prevent Officer will work closely with their Operational Prevent counterpart to ensure they are continually aligned to the practical manifestation of Cyber Prevent and the Prevent Network.

They will be responsible for drafting Policy for Cyber Prevention, ensuring a template founded on good governance is established to enable clarity and focus of this developmental project.

One of their key roles is to forge and maintain relationships with representatives from the private sector. They will promote the benefits of primarily the Digital and Financial sectors engaging with the Prevent programme. They will also work with academia to identify the areas within Prevent that require further research and empirical evidence to help clarify the local difference of pathways into cybercrime, if any.

The Strategic Prevent Officer will be based within the national cybercrime structures. They will be expected to report directly to the Senior Police officer who holds the Cyber Prevent portfolio.

Essential Criteria

- Experience of working with government departments
- Extensive public speaking ability and experience
- Excellent report/policy writing and interpersonal skills
- Comprehensive understanding of Cybercrime and current threats
- Willingness to travel domestically and internationally to fulfil duties

Continued...

Appendix

Appendix 2 – Cyber Prevention Officer - Strategy

Cybercrime Unit – Prevent Officer (Strategy) continued…

Core Responsibilities

- Work with government representatives to assist with the departmental development of Cyber Prevention Strategy and Policy
- Forge relationships with representatives from the private sector to develop Cyber Prevent initiatives and interventions
- Develop innovative and targeted national campaigns that raise societal awareness of pathways into cybercrime and digital opportunities in the legitimate world
- Draft Law enforcement protocols, policies and procedures which ensure delivery against the objectives of the Police Cyber Prevent strategy
- Forge and maintain relationships with key stakeholders i.e., gaming, academia, tech industry and on/off-line media to progress Prevent
- Assist in the development and consolidation of an international Cyber Prevent Network
- Work with the Operational Prevent Officer to focus contributions to National Prevent policies and to develop Law Enforcement processes and protocols.

International Prevent Network: The Prevent Officer will act as the Single Point of Contact (SPOC) for Prevent Officers established around the globe. They will focus on building a network within the countries in their region without compromise to fermenting relationships with Prevent Officers on other continents

Desirable Criteria

- Work with government representatives to assist with experience of working within the finance, gaming and/or digital industry
- Comprehensive understanding of cybercrime legislation
- Experience or understanding of neurodiversity
- Degree in Information Technology or similar subject, or Social Science (Criminology, Psychology etc)
- Understanding of cybercriminal career pathways
- Interest in gaming and related online forums

Appendix 3 – Cyber Prevention Officer - Operational

EXAMPLE

Jane Briggs

Cybercrime Unit – Prevent Officer (Operational)

The Prevent Officer's primary role is to work towards the Cyber Prevention aims and objectives within the National Cyber Security Strategy. They will raise public awareness of cybercrime in all its forms and identify opportunities for early intervention. They will identify vulnerable individuals at risk or involved in cybercrime. The officer, together with private and public sector partners, will be responsible for formulating strategies to amplify the impact of operations against the cybercrime fraternity.

The Prevent Officer will be based within the national cybercrime structures. They will be expected to identify operations in which Prevent intervention would amplify effectiveness by impacting on as many criminal actors as possible.

Essential Criteria

- Extensive public speaking ability and experience
- Excellent report writing and interpersonal skills
- Comprehensive understanding of cybercrime and current threats
- Comprehensive understanding of cybercrime legislation
- Willingness to travel domestically and internationally to fulfil duties

Continued...

Appendix

Appendix 3 – Cyber Prevention Officer - Operational

Cybercrime Unit – Prevent Officer (Operational) continued...

Core Responsibilities

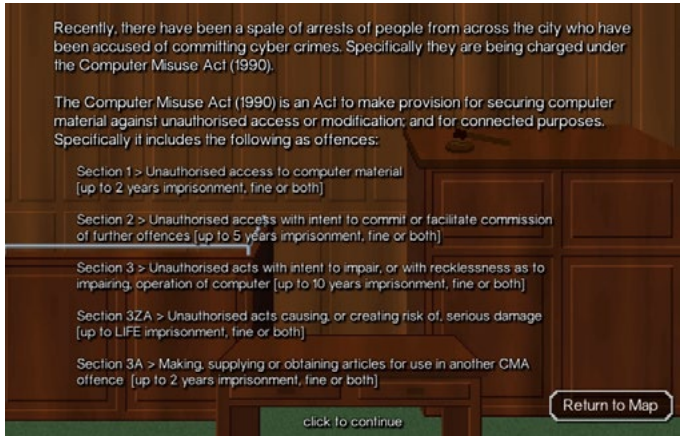
- Identify individuals subject to a Prevent or criminal justice intervention to debrief and inform cybercriminal career pathways
- Analyse intelligence and open-source information to identify and report on thematic trends
- Develop innovative and targeted campaigns that raise societal awareness of pathways into cybercrime and digital opportunities in the legitimate world
- Draft protocols, policies and procedures which ensure delivery against the objectives of the Cyber Prevent strategy
- Forge and maintain relationships with key stakeholders i.e., gaming, academia, tech industry and on/off-line media to progress Prevent
- Identify opportunities for Prevent interventions as part of all Cybercrime operations undertaken by the cybercrime unit
- Promote Prevent through publicity material and presentations to key target audiences and stakeholders
- Engage and upskill with established National Prevent Teams and Subject Matter Experts
- **Prevent Network:** The Prevent Officer will coordinate Single Points of Contact (SPOC) situated around Police Districts in-country, who will act as satellites for Prevent activities. This Prevent Network will comprise police officers who hold a Cyber Prevent portfolio that they manage alongside their normal duties.

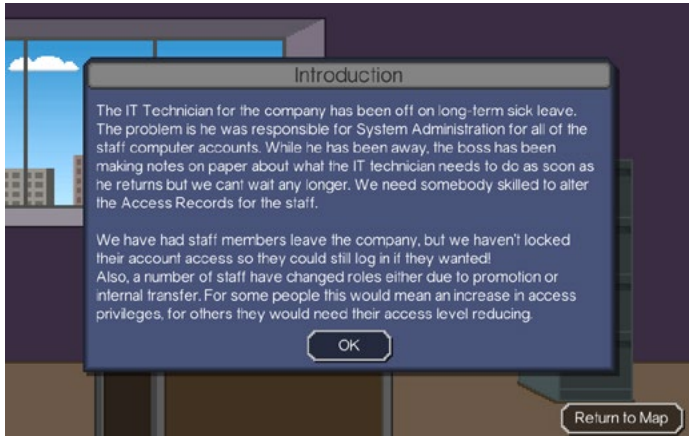
Desirable Criteria

- Experience of managing offenders
- Experience or understanding of neurodiversity
- Degree in Information Technology or similar subject, or Social Science (Criminology, Psychology etc)
- Understanding of criminal career pathways
- Interest in gaming and related online forums

Appendix

Appendix 4 – Images of the UK's CyberLand Challenge





Appendix

Appendix 5 – Image from SAP Africa Code Week (2021)

Appendix

Appendix 6 – Overview of Coding Lab Singapore Learning Roadmap (2021)

Ages 4-6

Animation | Robotics | Play Doh Circuits

Start your child on their journey in logical thinking – program an animation and direct a robot to retrieve treasure.

Ages 7-9

Scratch | Game Development | Young Computer Scientists

Beginning with Game Development, students master 12 research areas under our award-winning Young Computer Scientists programme.

Ages 10-12

App Development | Python | Advanced Computer Scientists

Let your child excel in Computational Thinking with our progressive learning roadmap which takes them through App Development, Micro:Bit and Python.

Ages 13-18

Python | Electives | C++

Be future-ready with our proprietary Python courses ranging from Math simulations to Artificial Intelligence and Data Analytics.

Academics

IB (Java) | GCE 'O' Level Computing

Taking Computer Science for the International Baccalaureate or GCE 'O' Level Computing? Ace the examinations with our specialised coaching program.

Special Programmes

Gifted Coders | Olympiad | Competitions

For students who wish to pursue specialised training in a particular area of interest. By Invitation Only.

Appendix

Appendix 6 – Overview of Coding Lab Singapore Learning Roadmap (2021)

Ages 4-6

Animation | Robotics | Play Doh Circuits

Start your child on their journey in logical thinking – program an animation and direct a robot to retrieve treasure.

Ages 7-9

Scratch | Game Development | Young Computer Scientists

Beginning with Game Development, students master 12 research areas under our award-winning Young Computer Scientists programme.

Ages 10-12

App Development | Python | Advanced Computer Scientists

Let your child excel in Computational Thinking with our progressive learning roadmap which takes them through App Development, Micro:Bit and Python.

Ages 13-18

Python | Electives | C++

Be future-ready with our proprietary Python courses ranging from Math simulations to Artificial Intelligence and Data Analytics.

Academics

IB (Java) | GCE 'O' Level Computing

Taking Computer Science for the International Baccalaureate or GCE 'O' Level Computing? Ace the examinations with our specialised coaching program.

Special Programmes

Gifted Coders | Olympiad | Competitions

For students who wish to pursue specialised training in a particular area of interest. By Invitation Only.

Table of Figures

References

References

[1] College of Policing. 2021. Disrupting serious and organised criminals: Menu of tactics. [online] Available at [Accessed 4 April 2021].

[2] Cybergamesuk.com. 2021. Cyber Games UK. [online] Available at: <https://cybergamesuk.com> [Accessed 15 April 2021].

[3] Europol, 2020. How COVID-19-related crime infected Europe during 2020. [online] Available at: < > [Accessed 4 April 2021].

[4] BBC News. 2017. Rehab for teenage hackers. [online] Available at: <https://www.bbc.co.uk/news/av/technology-40655656> [Accessed 15 April 2021].

[5] Forbes. 2016. Microsoft Co-Founder Bill Gates Was Caught Hacking 45 Years Ago. [online] Available at: <https://www.forbes.com/sites/stevemorgan/2016/02/18/microsoft-co-founder-bill-gates-was-caught-hacking-45-years-ago/?sh=4a16e6f8ba47.> [Accessed 4 April 2021].

[6] Hashed Out by The SSL Store™, 2020. Teen Hackers & Cybercrime: Teen Rebellion Ain't What It Used to Be - Hashed Out by The SSL Store™. [online] Available at: <https://www.thesslstore.com/blog/teen-hackers-cybercrime-teen-rebellion-aint-what-it-used-to-be> [Accessed 4 April 2021].

[7] International Finance Corporation. 2020. A New Study Explores Digital Skills in Sub-Saharan Africa. [pdf] Available at: <https://www.ifc.org/wps/wcm/connect/38390d15-e30e-4d6e-b0d2-bb09f6146efa/Digital+Skills+Report_Flyer_5-22-19_web.pdf?MOD=AJPERES&CVID=mHwcBU8> [Accessed 4 April 2021].

[8] INTERPOL, 2017. Global Cybercrime Strategy. [online] Available at [Accessed 4 April 2021].

[9] INTERPOL, 2021. Cybercrime. [online] Available at: <https://www.interpol.int/en/Crimes/Cybercrime> [Accessed 4 April 2021].

[10] INTERPOL, 2021. INTERPOL report charts top cyberthreats in Southeast Asia. [online] Available at: <https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia> [Accessed 4 April 2021].

[11] Judiciary.org.bd. 2020. Probation Services | Judicial Portal. [online] Available at: <http://www.judiciary.org.bd/en/probation-services> [Accessed 4 April 2021].

[12] Kshetri, N., 2019. Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, [online] 22(2), pp.77-81. Available at: <https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527> [Accessed 4 April 2021].

[13] Africacodeweek.org. 2021. AfricaCodeWeek. [online] Available at: <https://africacodeweek.org/tag/maroc/> [Accessed 15 April 2021].

[14] Aiken, M., Davidson, J., Amann, P., 2016. [online] Youth pathways into cybercrime. Available at: https://publikationen.uni-tuebingen.de/xmlui/bitstream/handle/10900/87701/pathways-white-paper.pdf?sequence=1 [Accessed 13 January 2021].

References

[15] Apolitical. 2019. Unlocking Africa's digital potential. [online] Available at: <> [Accessed 4 April 2021].

[16] BBC News. 2017. Rehab for teenage hackers. [online] Available at: <https://www.bbc.co.uk/news/av/technology-40655656> [Accessed 15 April 2021].

[17] Bill & Melinda Gates Foundation, 2021. CREST (INTERNATIONAL). [online] Available at: <https://www.gatesfoundation.org/about/committed-grants/2019/11/inv001323> [Accessed 4 April 2021].

[18] Revelock (2019), Teens and cybercrime: The reasons behind it, Corrales, Jose Carlos [online] Available at: Teens and cybercrime: the reasons behind it (revelock.com) [Accessed May 17, 2021]

[19] Caballero, A., Bashir, S. 2020. [online] Africa needs digital skills across the economy – not just the tech sector. Available at < > [Accessed 4 April 2021].

[20] Crane, C. 2020. Teen Hackers & Cybercrime: Teen Rebellion Ain't What It Used to Be. [online] Available at: < > [Accessed 4 April 2021].

[21] Caballero, A., Bashir, S. 2020. [online] Africa needs digital skills across the economy – not just the tech sector. Available at < > [Accessed 4 April 2021].

[22] CREST, 2021. 2021. CREST receives $1.4M grant to help build cyber security capacity in Africa and Asia to help increase safe access to digital financial services for the poor. [online] Available at: <https://www.crest-approved.org/2020/03/09/crest-receives-1-4m-grant-to-help-build-cyber-security-capacity-in-africa-and-asia-to-help-increase-safe-access-to-digital-financial-services-for-the-poor/index.html> [Accessed 4 April 2021].

[23] CPNI. 2021. Current Threats to National Security - Terrorism and Espionage | CPNI. [online] Available at: <https://www.cpni.gov.uk/threat-landscape> [Accessed 4 April 2021].

[24] Coding for Kids - Coding Lab. 2021. Coding Classes for Kids | Coding Lab - Singapore. [online] Available at: <https://www.codinglab.com.sg/our-classes/?gclid=Cj0KCQjwyN-DBhCDARIsAFOELTngEJkH39zkX8R9XYU26SU1271bqeKHB2JTI9lyNU_NrGdgxa6Eu_UaApWZEALw_wcB> [Accessed 15 April 2021].

[25] Lentz, S, A; Chaires, R H (2007). "The invention of Peel's principles: A study of policing "textbook" history". Journal of Criminal Justice 35: 69–79. doi:10.1016/j.jcrimjus.2006.11.016.

[26] Leukfeldt, R. and Holt, T., 2019. The Human Factor of Cybercrime. 1st ed. Routledge.

References

[27] Livingstone, S., Davidson, J., Bryce, J., Batool, S. 2017. Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group. Available at: < > [Accessed 4 April 2021].

[28] National Cyber Crime Unit Prevent Team, 2017. Pathways Into Cyber Crime. pp.1-18. Available at: <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file> [Accessed 4 April 2021]

[29] NCA/CREST, 2015. Identify, Intervene, Inspire: Helping Young People To Pursue Careers In Cyber Security, Not Cyber Crime. pp.2-10. Available at: <https://www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf> [Accessed 4 April 2021].

[30] Osborne, C. 2019. UK, EU police pilot scheme to give wayward teen hackers white hats. [online] Available at: [Accessed 4 April 2021].

[31] Oxford Dictionary, Lexico, 2021. [online] Available at: [Accessed 4 April 2021].

[32] Politie.NL. 2021. [online] Available at: <https://publicaties.politie.nl/changeyourgame/> [Accessed 15 April 2021].

[33] Pritchard, S. 2020. Hack_Right: Dutch cybercrime prevention program comes of age. The Daily Swig: Cybersecurity news and views. Available at < > [Accessed 4 April 2021 and 29 June 2021].

[34] Pshe-association.org.uk. 2020. Exploring Cybercrime: KS3 Lesson plans, the National Crime Agency (NCA). [online] Available at: <https://www.pshe-association.org.uk/curriculum-and-resources/resources/exploring-cybercrime-ks3-lesson-plans-national> [Accessed 4 April 2021].

[35] Raising Children Network. 2021. Digital citizenship: teens being responsible online. [online] Available at: <https://raisingchildren.net.au/pre-teens/entertainment-technology/digital-life/digital-citizenship> [Accessed 15 April 2021].

[36] Roddick, A., 2005. Business as unusual. Chichester: Anita Roddick Books. ISBN-10: 000710796X.

[37] SANS. 2019. SANS EMEA Survey: the iGen and Cyber Security: Is the next generation aware of Cyber Security's importance. [online] Available at: [Accessed 4 April 2020].

[38] The World Bank. 2018. [online] Preparing ICT Skills for Digital Economy: Indonesia within the ASEAN context. Available at <> [Accessed 4 April 2021].

[39] United Kingdom Crown Prosecution Service, 2021. Cybercrime - prosecution guidance | The Crown Prosecution Service. [online] Available at: <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> [Accessed 4 April 2021].

References

[40] United Nations: Office on Drugs and Crime. 2021. Crime Prevention. [online] Available at: <https://www.unodc.org/unodc/en/justice-and-prison-reform/CrimePrevention.html> [Accessed 4 April 2021].

[41] Waldrop, M., 2021. How to Hack the Hackers: The Human Side of Cyber Crime. [online] Scientific American. Available at: <https://www.scientificamerican.com/article/how-to-hack-the-hackers-the-human-side-of-cyber-crime/> [Accessed 4 April 2021].

[42] Youth Justice Board, 2019. Youth Justice Statistics 2018/2019 England and Wales. [online] Available at: [Accessed 4 April 2021].